ガウスの和 ポアンカレの和

数論の最前線から

Takashi Ono
小野 孝
［著］

日本評論社

はしがき

本書は2部と付録からなる．第1部は，『数学セミナー』1986年11月号から1987年4月号まで6回にわたって連載した「ガウスの和とルジャンドル多項式」をほとんどそのまま収録したものである．

事の起りは， 4年ほど前，亀井哲治郎さんから上記連載を単行本の形にしてはというお話があり，いろいろと心が揺れた．その頃ホプキンスの数学教室に楯辰哉さん(当時慶應大)が滞在しておられ，多様体上の調和解析の新進気鋭の数学者の立場からルジャンドル多項式の扱い方を私に教えてくださり，数論にも興味を持たれ，私の『数学セミナー』の上記連載の意味も理解しようと努められた．

も一つ，ハプニングがあった．1999年に『球面上の代数的組合せ理論』(シュプリンガー・フェアラーク東京)が坂内英一さん，坂内悦子さんにより著された．その導入を引用する：

> 「……この本の最初の3つの章で書いたことは，小野［356］の雑誌数学セミナーの連載記事(1986年11月号から1987年4月号まで)での主題の取り扱いと非常に近いものがある．(中略)　我々がこの連載記事を知ったとき(1988年頃)，これらの主題に関して書きためてあった我々の原稿の数学的内容との類似に驚いたことを覚えている．しかしこれは偶然ではないのである．小野の記事においては，球面上の調和解析と，有限体上の調和解析ともいえるガウス和などとの関連性が主題であった．この有限体上の調和解析は，アソシエーションスキームの上の表現論(調和解析)の特別な一例であるからである．……」

これで亀井さんのお誘いに心が揺れたわけもお分かりでしょう．一方では，

楯さんや坂内さんご夫妻のお仕事に触発されて，もっと現代的な「ガウスの和とルジャンドル多項式」(増補改訂版)を書いてはという気持になったのであるが，他方この5年ほど前からずっとポアンカレの和の話，すなわち保型関数論のポアンカレ級数に触発された整数論(とくにガロア・コホモロジーや野性的(wild)分岐理論)が頭から離れず，第2部として第1部と独立な「ポアンカレの和」を加えることに決めたのである．第1部と第2部には通底した主題があるのだが，それをひと目で見るために下の大変大雑把な仕上がったクロスワード・パズルが少しはお役に立つと思う．

	第1部	第2部
人物	ルジャンドル(1752−1833) ガウス(1777−1855)	ポアンカレ(1854−1912) ヒルベルト(1862−1943)
概念	群，環，体	コホモロジー

[付録について]

付録2「方程式を解くことについて」は『数学セミナー』1985年9月号，10月号の記事を収録したもので，これがきっかけとなって「ガウスの和とルジャンドル多項式」の連載(1986年11月号から1987年4月号まで)が始まった．付録1は『数学セミナー』1991年10月号の記事の収録で，いずれも本論(第1部，第2部)のアペリチフないしリキュールと思ってくだされば幸いである．

付録3は，本論第2部の英訳ではない．少し拡張された系(system)の上での第2部の展開のsketchをコンピュータからそのまま引っ張り出したものである．

2007年11月　　ボルチモア

小野　孝

目次

第2部　ポアンカレの和

付録

第1部

ガウスの和とルジャンドル多項式


ガウス(1777-1855)


ルジャンドル(1752-1833)

第1回

球面上の多項式
初等整数論とは何か?
mod p のフーリエ解析

昨年(1985年)5月，立教大学での公開講演「方程式を解くことについて」[0)]をまとめて『数学セミナー』(1985年9, 10月号)に載せていただいたのがきっかけで，表記の題で連載を書くことになった．私にこのような機会が与えられたことを大変ありがたく思う．『数学セミナー』ののびのびした楽しい雰囲気をこわさないように私もできるだけ工夫したい．

ご承知のようにガウスの和は数論($\mathbb{Z}, \mathbb{F}_p = \mathbb{Z} \bmod p$)に，ルジャンドル多項式は解析($\mathbb{R}, \mathbb{C}$)に出てきて，一見何の関係もないように見える．しかし，多くの昔の偉い人々がそうであったように，ガウスもルジャンドルもともに数論と解析の両方に通じていたのである．これは彼らが後年，定式化された群，環，体などの概念を感覚として持っていたからに違いないと思われる．我々はもうこれらの概念に慣れているから$\mathbb{F}_p$や$\mathbb{R}$もともに体であるという立場から見られるわけで，たとえば，ガウスの和とガンマ関数が同じ考え方で定義されていることに気がつくであろう．このような気持ちで18, 19世紀に美しく，華麗に展開された数論と解析のいくつかの部分を20世紀の立場から見直してみようというのが目標である．§1の後半部は予告編的意味もあり，あまり細部にこだわらずに読んでいただきたい．

対象が大学の1～2年程度とのことで，私も大学の教師をしている関係上いくらか感じがわかるが，数学の講義というものはまことにやりにくい．私とし

0） 本書に付録2として収録.

ては，独り言をいうほど極端ではないが，気心の知れた 4〜5 人の学生に研究室の小黒板の前で説明し，途中で脱線または立往生するのもまた楽し，といった気分でやりたい．

§1．球面上の多項式

$\mathbb{R}$ を実数体，$\mathbb{R}^n$ を n 次元のベクトル空間とする．S^{n-1} で単位球をあらわす：

$$S^{n-1} = \{ x \in \mathbb{R}^n ; Nx = {x_1}^2 + \cdots + {x_n}^2 = 1 \}.$$

$n=2$ なら S^1 は平面 $\mathbb{R}^2$ の単位円，$n=3$ なら S^2 は空間 $\mathbb{R}^3$ の単位球である．S^{n-1} 上の $\mathbb{R}$ に値をとる関数というのは

$$f : S^{n-1} \longrightarrow \mathbb{R}$$

なる任意の写像のことであるが，S^{n-1} 上の‘多項式’はどのようなものとして定義したらよいだろうか？　これを出発点の問題としよう．

$n=2$ としてみよう．問題は，単位円上の‘多項式’の定義である．答は簡単である．まず全平面上の多項式とは写像

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}$$

で

$$f(x, y) = \sum_{\lambda, \mu} a_{\lambda\mu} x^\lambda y^\mu,$$

$$a_{\lambda\mu} \in \mathbb{R}, \qquad 0 \leqq \lambda \leqq \alpha,\ 0 \leqq \mu \leqq \beta$$

と 2 変数 x, y の多項式であらわされるものである[1)]．そうすれば S^1 は $\mathbb{R}^2$ の部分集合であるから，多項式

$$f : \mathbb{R}^2 \longrightarrow \mathbb{R}$$

を S^1 に制限した写像

$$f|_{S^1} : S^1 \longrightarrow \mathbb{R}$$

1）　厳密には‘多項式’と‘多項式写像’を区別すべきであろうが，ここでは省略する．

を S^1 上の‘多項式’とよぶのは自然であろう．以下この定義を採用することにする．$P(\mathbb{R}^2)$, $P(S^1)$ でそれぞれ $\mathbb{R}^2$, S^1 上の多項式の全体をあらわすと，これらは容易にわかるように環になる．つまりそこで多項式の和，差，積がとれる．

制限の写像

$$\rho : f \longmapsto f|_{S^1}$$

は定義から環の全射準同型写像になる：

$$P(\mathbb{R}^2) \longrightarrow P(S^1) \longrightarrow 0.$$

また，

$$\mathrm{Ker}\,\rho = \{ f \in P(\mathbb{R}^2) \,;\, f(S^1) = 0 \}$$

は $P(\mathbb{R}^2)$ のイデアルになる．すなわち次の完全系列ができる：

$$0 \longrightarrow \mathrm{Ker}\,\rho \longrightarrow P(\mathbb{R}^2) \longrightarrow P(S^1) \longrightarrow 0,$$

$$f|_{S^1} = g|_{S^1} \iff f \equiv g \pmod{\mathrm{Ker}\,\rho}$$

というわけである．さて，このような定義を任意の n に拡張することは容易だから，しばらく $n = 2$ のまま進もう．

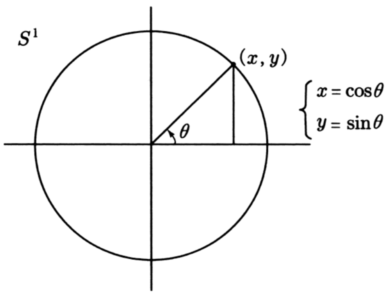


図1

単位円 S^1 は1次元であるから1つのパラメータで定まる．図1のように角 θ をとるのが自然である．S^1 上の関数は θ の関数になるから多項式も θ の関数になる．

$$f(x, y) = \sum_{\lambda,\mu} a_{\lambda\mu} x^{\lambda} y^{\mu}$$

の x, y に $x = \cos\theta$，$y = \sin\theta$ を代入して得た θ の関数 $F(\theta)$ が $P(S^1)$ の

多項式の一般形となる：

(1) $$F(\theta)=f(\cos\theta,\sin\theta)=\sum_{\lambda,\mu}a_{\lambda\mu}\cos^{\lambda}\theta\sin^{\mu}\theta.$$

つまり，$P(S^1)$ の多項式とはいわゆる‘3 角多項式’にほかならない．ここで

$$\cos\theta=\frac{e^{i\theta}+e^{-i\theta}}{2},\qquad \sin\theta=\frac{e^{i\theta}-e^{-i\theta}}{2i}$$

とおいて 2 項定理を用いて $\cos^{\lambda}\theta, \sin^{\mu}\theta$ を指数関数であらわし，(1) に代入すると，

(2) $$F(\theta)=\sum_{\nu\in\mathbf{Z}}c_\nu e^{i\nu\theta},\qquad c_\nu=0\quad(|\nu|\geqq N)$$

と書きあらわされる．今度は係数 c_ν は複素数になる．(2) は有限項しかないが，

(3) $$g(\theta)=\sum_{\nu\in\mathbf{Z}}c_\nu e^{i\nu\theta}$$

とあらわされる S^1 上の関数を考えれば，g は S^1 上の多項式の極限になる関数，すなわちフーリエ展開可能な関数にほかならない[2)]．本稿ではフーリエ級数論には立ち入らず，その一歩手前の多項式 (2) に集中するとして，S^1 の代りに球面 S^2 を用いたら (2) はどんなものに変わるかということを調べて見よう．

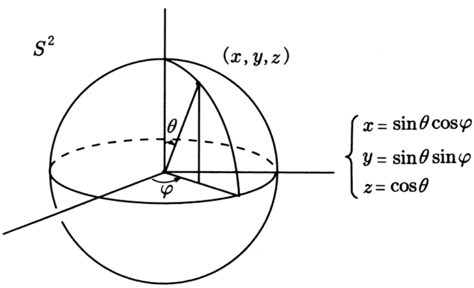


図 2

2） $P(\mathbb{R}^2), P(S^1)$ の多項式の係数は $\mathbb{R}$ に限ったが，このような文章を正当化するには，変数は $\mathbb{R}$ でも係数は $\mathbf{C}$ にとっておいた方が安全である．

$P(\mathbb{R}^3), P(S^2)$ は $n=2$ の場合と同様に定義されるが，単位球は2次元だから2つのパラメータをもつ．図2のように角 θ, φ をとるのが自然である．

$$f(x, y, z) = \sum_{\lambda,\mu,\nu} a_{\lambda\mu\nu} x^\lambda y^\mu z^\nu \in P(\mathbb{R}^3)$$

の x, y, z に

$$x = \sin\theta\cos\varphi, \qquad y = \sin\theta\sin\varphi, \qquad z = \cos\theta$$

を代入して得た θ, φ の関数 $F(\theta, \varphi)$ が $P(S^2)$ の多項式の一般形となる：

$$(4) \qquad F(\theta, \varphi) = f(\sin\theta\cos\varphi, \sin\theta\sin\varphi, \cos\theta)$$

$$= \sum_{\lambda,\mu,\nu} a_{\lambda\mu\nu} \sin^{\lambda+\mu}\theta\cos^\nu\theta\cos^\lambda\varphi\sin^\mu\varphi.$$

ここから直ちに $n=2$ のように，すべてを指数関数で書くと何のことかわからなくなる．$P(S^2)$ を正しく把握するために次のように考える．まず通常の $\mathbb{R}^3$ 上の多項式環を

$$(5) \qquad P(\mathbb{R}^3) = \bigoplus_{l=0}^{\infty} P_l(\mathbb{R}^3), \qquad P_l(\mathbb{R}^3) = l \text{ 次の斉次式の空間}$$

にわける．次にラプラシアン

$$\Delta = \left(\frac{\partial}{\partial x}\right)^2 + \left(\frac{\partial}{\partial y}\right)^2 + \left(\frac{\partial}{\partial z}\right)^2$$

を用いて

$$(6) \qquad H(\mathbb{R}^3) = \{ f \in P(\mathbb{R}^3) ; \Delta f = 0 \} = \bigoplus_{l=0}^{\infty} H_l(\mathbb{R}^3),$$

$$H_l(\mathbb{R}^3) = H(\mathbb{R}^3) \cap P_l(\mathbb{R}^3)$$

によって調和多項式，l 次の調和形式の空間を定義すると面白いことに，全射

$$\rho : P(\mathbb{R}^3) \longrightarrow P(S^2) \longrightarrow 0$$

を $H(\mathbb{R}^3)$ に制限しても全射になる：

$$(7) \qquad \rho|_H : H(\mathbb{R}^3) \longrightarrow P(S^2) \longrightarrow 0.$$

つまり，球面上の多項式はすべて調和多項式から得られる．そして $\rho|_H$ をさらに l 次の部分に制限すると，$H_l(S^2)$ を $H_l(\mathbb{R}^3)$ の $\rho|_H$ による像としたとき，同型対応

$$(8) \qquad H_l(\mathbb{R}^3) \approx H_l(S^2)$$

および直和分解

$$(9) \qquad P(S^2) = \bigoplus_{l=0}^{\infty} H_l(S^2)$$

が成り立ち，次の $2l+1$ 個の S^2 上の多項式

$$(10) \qquad \begin{cases} P_l(\cos\theta), \\ \cos m\varphi \sin^m\theta\, P_l^{(m)}(\cos\theta), \\ \sin m\varphi \sin^m\theta\, P_l^{(m)}(\cos\theta), \qquad 1 \leqq m \leqq l \end{cases}$$

が $H_l(S^2)$ の底になる[3]．ここに $P_l(t)$ は**ルジャンドル多項式**で

$$P_l^{(m)}(t) = \left(\frac{d}{dt}\right)^m P_l(t)$$

である．$P_l(t)$ の定義は

$$(11) \qquad P_l(t) = \frac{1}{2^l l!}\left(\frac{d}{dt}\right)^l (t^2-1)^l, \qquad l \geqq 0.$$

これで表題にあらわれるガウスとルジャンドルのうち 1 人が登場した．

(5)－(10) およびその任意の n への拡張は節を追って検討しなければならないが，$n=2$ も入れていえば，円，球面，3 次元の球面，4 次元の球面，……に対して多項式の概念を導入し，その空間の底を，球面たちを，表示するパラメータで上手にあらわすことは純代数的な問題であり，フーリエが‘すべての関数を 3 角関数で書いて見せる！’と豪語した意味でのフーリエ解析の真意は，すでに多項式の段階に現れていることに気がつくのである．どんな関数がフーリエ展開できるかといった問題は第二義的な問題である．要するにフーリエ展開できる関数というのが大切な概念であって，やはり(ℝ 上の)多項式の極限であるテーラー級数がそれだけで大切な概念であるのと似ている．

3） $n=2$ の場合にも (5)－(10) に相当する手続きを踏むことができる．そのとき $P_l(t)$ に相当するものは

$$P_l(t) = \cos(l \cos^{-1} t)$$

となる．これはチェビシェフの多項式である．$n \geqq 3$ もこめていえば，一般に，ここに現れる多項式は超幾何多項式(Hypergeometric polynomial)である．

§2．初等整数論とは何か？

私の勤めている大学では年に3ヵ月(セメスターといい年2学期，秋と春，のうちの1つ)「初等整数論」の講義をすることになっている．これは教える方も学ぶ方も予備知識がいらないのでいろいろな人が入れ替り立ち替り講義をする．それで私も5年に一度くらいはこの講義をする．学生ははじめのうちは30人ほどいるがセメスターの終りには20人くらいになる．普通週3回(月，火，水)で1回は50分，それと大学院生が世話をする演習が週1回ある．院生は宿題のチェックをしたり質問に答えたりする．また，ある孤立した話題について講義をしてくれることもある．

今年(1986年)はちょうど私にこの講義の番が来た．教科書をきめなければならない．ある風変りな学校があって，幾何はユークリッドの『原論』，力学はニュートンの『プリンキピア』と何でもその方面の最初の古典を教科書にするそうだが，私もガウスの《Disquisitiones arithmeticae(整数論講究)》を教科書にしてみようかとなかば本気で考えたのだが，やめた．ガウスの『整数論』の主要部分は $\mathbb{Z}$ 係数の2元2次形式

$$ax^2+2bxy+cy^2$$

の徹底した分類論である．群の概念のまだなかった時代に，与えられた判別式を持つ2次形式の類(class)が合成(composition)により有限アーベル群 H となり，2次形式の種(genus)が H の指標(character)により定まることを証明したのは驚くべきことである[4)]．このような本を教科書に使ったら教師，生徒が共倒れになることは目に見えているので，やめたのである．ただ図書館に行ってガウスの本の序文だけは読んでくるように学生に伝えておいた．序文の中ほどに次のように書いてある．

「たまたま私は驚くべき算術的真理に行き当った[5)]．私はそれをたいそう

4）　この本の印刷は1798年に始まったそうだから，ガウスはせいぜい21歳であった．(ゲッチンゲン)大学1〜2年程度にこのような学生がいたのである．

美しいと思い，もっと深い事柄[6]との関連に気づいたので，それの基づく原理を理解し厳密な証明を得ることに全力を集中した．このようにして次から次へと結果が出て来て，他の先達[7]の残した仕事を学ぶ前にこの本の最初の 4 章[8]をほとんど書きあげた」

さて，私は，ガウスがいう最初の 4 章すなわち合同式から相互律までをいちおう「初等整数論」と考えたいと思う．私が採用した教科書は 2 冊で，いずれも 100 ページにも満たない小さなものである：

［W］ A. Weil, Numder Theory for Beginners, Springer，第 2 刷，1985.

［B］ A. Baker, A Concise Introduction to the Theory of Numbers, Cambridge Univ. Press., 1984.

私は［W］を正，［B］を副とし，前者に沿って講義をし，後者は自習用の読本として自由に読むように学生に薦めておいた．［W］は 13 節からなり，次のようである．これも「初等整数論とは何か？」への 1 つの答えであり，ガウスの最初の 4 章と大差はない．［W］の各節(§)は§Ⅰ，§Ⅱ，……，§XIIIと羅馬(ローマ)数字があるだけで表題がないので私が適当に附け加えておく．

§Ⅰ　数学的帰納法

§Ⅱ　最大公約数とユークリッドの互除法

§Ⅲ　1 次方程式 $ax+by+\cdots+cz=d$

§Ⅳ　整数論の基本定理(素因数分解の一意性)

§Ⅴ　合同 $x\equiv y \pmod{m}$

§Ⅵ　環 $\mathbb{Z}/m\mathbb{Z}$ と群 $(\mathbb{Z}/m\mathbb{Z})^\times$

§Ⅶ　有限巡回群

§Ⅷ　フェルマ - オイラーの定理

5）　奇素数 p について，

$$x^2\equiv -1\,(p)\text{ がとける} \iff p\equiv 1\,(4)$$

6）　相互律.

7）　フェルマ，オイラー，ラグランジュ，ルジャンドルの 4 人.

8）　数の合同，1 次合同式，巾剰余，2 次合同式，相互律.（5)～8) は筆者註)

§IX　多項式環 $K[X]$

§X　$(\mathbb{Z}/p\mathbb{Z})^{\times}$ は巡回群になること(原始根 mod p の存在)

§XI　巾剰余の定義

§XII　平方剰余の相互律

§XIII　ガウスの整数環 $\mathbb{Z}[i]$ と $x^2+y^2=p$ の解

[W] では，初等整数論を群，環，体に馴染むための絶好の実例と見る態度があり，たいへんよい．今日では，大学1〜2年生にとって群，環，体はほとんど常識である[9]．そして§VIIIのフェルマ - オイラーの定理[10]を任意の有限群に関する簡単な定理の極めて特別な場合に過ぎない，と捉えるのは群論的考え方の勝利である．同様に§Xの原始根の存在も任意の体 K の乗法群 $K^{\times}$ の有限部分群は巡回群であるという一般的事実の極めて特別な場合として扱われている．

ところで，いくら群，環，体をふりまわしてもどうにもならないのが相互律である．[W] の証明はガウス自身の第3証明と実質的に同一で初等的ではあるが，この本の他の部分に較べてアクロバティク(軽業的)であるので，私は，少し長くなるが，長い目で見ればはるかに含蓄のある**ガウスの和**による証明におきかえた．

そこで後続の2〜3回では，このガウスの和による相互律の証明を目標にしようと思う．その前に [B] について少し書いておく．[B] は [W] のコンパクトなスタイルと反対に，2元2次形式，ディオファントス近似，連分数，ディオファントス方程式(Faltings も出てくる)も含みにぎやかである．また，いわゆる初等整数論特有の open problems で読者を興奮させることも忘れていない：

(i)　フェルマの素数，

(ii)　メルセンヌの素数，

(iii)　ゴールドバッハの予想，

9）ガウスが学生の頃は群，環，体は誰も知らなかった．‘知らない方がよかったのだ’などといわないでください．

10）$x \in \mathbb{Z},\ (x, m)=1 \implies x^{\varphi(m)} \equiv 1 \pmod{m}$.

(iv)　双子の素数，

(v)　リーマン予想，

(vi)　奇の完全数，

(vii)　オイラーの定数の超越性，

(viii)　$\zeta(2n+1)$ の超越性，

(ix)　フェルマの予想，

(x)　カタランの予想．

私も，万一をおもんぱかって，もし諸君の中にこれらの open problems に有意義な寄与をした者がいれば，学期末試験を免除したうえ A^+ をあげると宣言しておいたが，何事も起こらなかった[11)]．

§3．mod p のフーリエ解析

単位円 S^1 上の多項式の極限になる関数，すなわちフーリエ展開可能な関数 g は§1の (3) により

(1)　$$g(\theta)=\sum_{\nu\in\mathbf{Z}}c_\nu e^{i\nu\theta},\qquad c_\nu\in\mathbf{C}$$

と書けていた．ここで大切なのは

(2)　$$\chi_\nu(\theta)=e^{i\nu\theta},\qquad \nu\in\mathbf{Z}$$

とおくと χ_ν は S^1 から$\mathbf{C}^\times$ (複素数の乗法群)への準同型写像であり，χ_ν の直交性：

(3)　$$\langle\chi_\nu,\chi_\mu\rangle=\frac{1}{2\pi}\int_0^{2\pi}\chi_\nu\bar{\chi}_\mu d\theta=\frac{1}{2\pi}\int_0^{2\pi}e^{i(\nu-\mu)\theta}d\theta=\delta_{\mu\nu}$$

によってフーリエ係数 c_ν が

11)　ここにあげた予想 (i)—(x) のうち (ix)，(x) はその後(すなわち 1985 年以降)証明された．

$$(4) \qquad \langle g, \chi_\nu \rangle = \frac{1}{2\pi}\int_0^{2\pi} g\bar{\chi}_\nu d\theta = \sum_\mu c_\mu \langle \chi_\mu, \chi_\nu \rangle = c_\nu$$

によって計算されることである．これだけの形式的手続きならば，単位円 S^1 を任意の有限アーベル群 G でおきかえてもできる．そこで G を位数 N の有限アーベル群とし，G の上で定義され $\mathbb{C}$ に値をもつ関数全体を $L(G)$ と書こう．$f, g \in L(G)$に対して

$$(f+g)(x) = f(x)+g(x),$$

$a \in \mathbb{C}$ に対して

$$(af)(x) = af(x)$$

とすることにより，$L(G)$ は $\mathbb{C}$ 上のベクトル空間になる[12)]．

命題 1　G が位数 N のアーベル群ならば，$L(G)$ は N 次元である．

証明　G の 1 点 y の特性関数 f_y を

$$f_y(x) = \delta_{xy} = \begin{cases} 1, & x = y \\ 0, & x \neq y \end{cases}$$

で定義すれば $\{f_y\}_{y \in G}$ が $L(G)$ の底(basis)になることがわかる．まず，任意の $f \in L(G)$ は

$$f = \sum_y f(y) f_y$$

と書けるから $\{f_y\}$ は $L(G)$ を張る．次に

$$\sum_y a_y f_y = 0$$

とすると，この両辺を G の任意の x で値をとって

$$a_x = 0$$

が出る．すなわち $\{f_y\}$ は独立である，Q.E.D.

ここで $L(G)$ に次のように内積を定義する：

12)　積も自然に定義できて $L(G)$ は環になるが，ここでは考えないことにする．

(5) $$\langle f, g\rangle = \frac{1}{N}\sum_{x\in G} f(x)\bar{g}(x), \qquad f, g \in L(G)$$

ただし，$\bar{g}(x) = \overline{g(x)}$．すると

(6) $$\begin{cases} \langle f+g, h\rangle = \langle f, h\rangle + \langle g, h\rangle, \\ \langle af, g\rangle = a\langle f, g\rangle, \\ \langle g, f\rangle = \overline{\langle f, g\rangle}, \qquad \langle f, f\rangle \geqq 0, \\ \langle f, f\rangle = 0 \iff f = 0 \end{cases}$$

が成り立つ．すなわち命題 1 とあわせて，

> **定理 1** G を位数 N の有限アーベル群とすると，$(L(G), \langle\ ,\ \rangle)$ は N 次元のヒルベルト空間になる．

次に，**指標** χ，すなわち

$$\chi : G \longrightarrow \mathbb{C}^{\times}$$

なる準同型写像を考える．G が有限群だから

$$x^N = e, \qquad e \text{ は } G \text{ の単位元}$$

で，この両辺に χ をほどこすと

$$1 = \chi(x^N) = \chi(x)^N$$

だから $\chi(x)$ の値は 1 の N 乗根で，

$$|\chi(x)|^2 = \chi(x)\bar{\chi}(x) = 1$$

である．2 つの指標 χ, χ' の積を

$$(\chi\chi')(x) = \chi(x)\chi'(x)$$

によって定義すると，$\chi\chi'$ はまた指標になることが確かめられる．

$$\varepsilon(x) = 1, \qquad x \in G$$

で定まる ε を単位指標という．すると指標の全体 $\widehat{G}$ は群になる．$\widehat{G}$ を G の**指標群**という．明らかに

$$\chi^{-1} = \bar{\chi}$$

である．また

$$\widehat{G} \subset L(G)$$

である．

定理 2　$\widehat{G}$ はヒルベルト空間 $(L(G), \langle\ ,\ \rangle)$ の正規直交底になる．

証明　まず G が巡回群の場合，

$$G = \langle g \rangle$$

と生成元であらわすと

$$\mathbb{Z} \ni \nu \longmapsto \chi_\nu : \chi_\nu(g) = e^{(2\pi i/N)\nu}$$

によって同型対応

$$\mathbb{Z}/N\mathbb{Z} \approx \widehat{G}$$

が得られるので，$\widehat{G}$ も G と同じ位数の巡回群になる．G が一般のアーベル群の場合には，

$$G = G_1 \times \cdots \times G_l$$

と巡回群の直積にわけられるから，

$$\widehat{G} \approx \widehat{G}_1 \times \cdots \times \widehat{G}_l$$

に注意すれば $\widehat{G}$ も G と同じ位数の(事実 G と同型な)群になる．以上から $\widehat{G}$ は $L(G)$ の次元 N だけの要素をもつことがわかった．

ここで $\chi \in \widehat{G}$ が次の大切な性質をもつことを見ておこう：

$$(7) \qquad \sum_{x \in G} \chi(x) = \begin{cases} N, & \chi = \varepsilon, \\ 0, & \chi \neq \varepsilon. \end{cases}$$

実際，この左辺の和を A と書くと，

$$A = \sum_x \chi(x) = \sum_x \chi(xy) = \sum_x \chi(x)\chi(y) = \chi(y)A$$

が任意の $y \in G$ に対して成り立つが，$\chi \neq \varepsilon$ なら $\chi(y) \neq 1$ なる y があるから $A = 0$ となる．一方，$\chi = \varepsilon$ なら $A = N$ は明らかである：

さて (7) を使うと次の直交性が出る：

$$(8) \qquad \langle \chi, \chi' \rangle = \begin{cases} 1, & \chi = \chi', \\ 0, & \chi \neq \chi'. \end{cases}$$

実際，

$$\langle \chi, \chi' \rangle = \frac{1}{N} \sum_x \chi(x) \bar{\chi}'(x)$$

$$= \frac{1}{N}\sum_{x}(\chi\bar{\chi}')(x) = \begin{cases} 1, & \chi\bar{\chi}' = \varepsilon, \\ 0, & \chi\bar{\chi}' \neq \varepsilon. \end{cases}$$

ここで $\bar{\chi}' = (\chi')^{-1}$ に注意すれば (8) になる．(8) から $\{\chi\}_{\chi\in\hat{G}}$ が独立なことはすぐ出る：

$$0 = \sum_{\chi} c_\chi \chi$$

ならば，任意の χ' について

$$0 = \langle 0, \chi' \rangle = \sum c_\chi \langle \chi, \chi' \rangle = c_{\chi'}$$

だから，Q.E.D.

以上から，任意の関数 $f \in L(G)$ は正規直交底 $\{\chi\}_{\chi\in\hat{G}}$ を用いて**フーリエ展開**されることがわかった：

(9) $$f = \sum_{\chi} c_\chi \chi, \qquad c_\chi = \langle f, \chi \rangle.$$

有限群 G から出発すればすべてが(級数，積分が)有限和だから収束の心配は全くない．‘任意の関数’ がフーリエ展開できたのである．

さて，表題にいう mod p のフーリエ解析を説明しよう．p を素数として有限体

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$$

を考える．体は加法と乗法をもっているから 2 つの有限アーベル群をもっている．加法群を $\mathbb{F}_p{}^+$，乗法群を $\mathbb{F}_p{}^\times$ であらわす．後者には $\{0\}$ が抜けているだけだから位数はそれぞれ p と $p-1$ である．$L(\mathbb{F}_p{}^+), L(\mathbb{F}_p{}^\times)$ はそれぞれヒルベルト空間で，$\widehat{\mathbb{F}_p{}^+}, \widehat{\mathbb{F}_p{}^\times}$ がそれぞれの正規直交底になっていて，各空間の関数はフーリエ展開を持つ．

$$\mathbb{F}_p{}^+ \supset \mathbb{F}_p{}^\times$$

だから $\mathbb{F}_p{}^+$ 上の関数を $\mathbb{F}_p{}^\times$ に制限すれば $\mathbb{F}_p{}^\times$ 上の関数が得られる．制限する写像を ρ と書くと完全系列：

$$0 \longrightarrow \mathrm{Ker}\,\rho \longrightarrow L(\mathbb{F}_p{}^+) \xrightarrow{\rho} L(\mathbb{F}_p{}^\times) \longrightarrow 0$$

が生じ，Ker ρ は $\mathbb{F}_p{}^\times$ のすべての点で 0 になる(原点 0 では任意に与えられた

値をとる)関数の全体から成る．加法的指標 $\psi \in \widehat{\mathbb{F}_p{}^+}$ を $\mathbb{F}_p{}^\times$ に制限して，乗法的指標 $\{\chi\}_{\chi \in \widehat{\mathbb{F}_p{}^\times}}$ によってフーリエ展開するとどうなるか？

(10)　$$\rho(\psi) = \sum_{\chi} c_\chi \chi, \qquad c_\chi = \langle \rho(\psi), \chi \rangle.$$

実はわれわれはこれに似たことを経験している．それは指数関数 e^x のテーラー展開である：

(11)　$$e^x = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots\cdots + \frac{1}{n!}x^n + \cdots\cdots.$$

ここで，

$$\psi(x) = e^x, \qquad \chi_n(x) = x^n$$

とおけば

$$\psi(x+y) = \psi(x)\psi(y), \qquad \chi_n(xy) = \chi_n(x)\chi_n(y)$$

で，ともかく一種の‘フーリエ展開’で $\dfrac{1}{n!}$ が χ_n の係数である．

$$n! = \Gamma(n+1)$$

だから (10) から生ずる関数

$$\chi \longmapsto c_\chi$$

も mod p の‘ガンマ関数’ではなかろうか？　このような粗雑な考察もそのうちに正当化される．

e^x の mod p の類似が

$$\zeta^x, \qquad \zeta = e^{2\pi i/p}$$

であることは論をまたない．より一般に $\mathbb{F}_p{}^+$ は次の意味で自己相対的である：

(12)　$$\mathbb{F}_p{}^+ \xrightarrow[\sim]{\psi} \widehat{\mathbb{F}_p{}^+}, \qquad \psi_\xi(x) = \zeta^{\xi x}, \quad \xi, x \in \mathbb{F}_p{}^+.$$

(12) の記号を用いれば (10) のフーリエ係数は：

(13)　$$c_\chi = \langle \rho(\psi_\xi), \chi \rangle = \frac{1}{p-1} \sum_{x \in \mathbb{F}_p{}^\times} \zeta^{\xi x} \bar{\chi}(x)$$

と与えられる．そこで $p-1$ で割ることをやめ，$\bar{\chi}$ と共役をとることもやめて次の定義をする：

定義１　p を素数，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ を有限体，$\zeta = e^{2\pi i/p}$, $\xi \in \mathbb{F}_p$, $\chi \in \widehat{\mathbb{F}_p{}^\times}$ に対して

$$(14)\qquad \tau_\xi(\chi) \overset{\text{def}}{=} \sum_{x \in \mathbb{F}_p{}^\times} \chi(x)\zeta^{\xi x}$$

とおき，ξ, χ に関する**ガウスの和**とよぶ．

とくに，$\tau_1(\chi) = \tau(\chi)$ とおく：

$$\tau(\chi) \overset{\text{def}}{=} \sum_{x \in \mathbb{F}_p{}^\times} \chi(x)\zeta^x.$$

ガンマ関数（オイラー第２種積分） $\Gamma(s) = \int_0^\infty e^{-x}x^s \frac{dx}{x}$	ガウスの和 $\tau(\chi) = \sum_x \chi(x)\zeta^x$
ベータ関数（オイラー第１種積分） $B(p,q) = \int_0^1 x^{p-1}(1-x)^{q-1}dx$ $= \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}$	ヤコビの和 $J(\chi, \chi') = \sum_x \chi(x)\chi'(1-x)$ $= \frac{\tau(\chi)\tau(\chi')}{\tau(\chi\chi')}$

表題にあるガウスの和とルジャンドル多項式が両方とも登場したので，今回はこの辺で切り上げようと思う．上の表は仕上がったクロスワード・パズルです．タテのカギ，ヨコのカギは何でしょう？

第2回

2次合同式
ガウスの相互律
正17角形の作図

前回のおわりに**ガウスの和**を定義した．今回の目標は§2で述べた‘初等整数論’で最も大切な**ガウスの相互律**のガウスの和による証明である．前回ではガウスの相互律が何であるかは説明しなかったので，今回は相互律の基礎にある2次合同式の説明から始めることにしよう．

§4．2次合同式

K を任意の体とし，

$$K^{\times} = K-\{0\}$$

を K の乗法群とする．$a, b, c \in K$ に対して

$$ax+b, \qquad a \neq 0$$

が一般の1次式で，

$$ax^2+bx+c, \qquad a \neq 0$$

が一般の2次式である．1次方程式

(1) $\qquad ax+b = 0$

の解はただ1つで，もちろん $x = -b/a$ で与えられる．2次方程式

(2) $\qquad ax^2+bx+c = 0$

を任意の体 K で解く場合には体 K の個性が問題となる．たとえば

$$K=\mathbb{R}\ (\text{実数体}),\qquad K=\mathbb{C}\ (\text{複素数体})$$

で事情が全く違う；$x^2+1=0$ が $\mathbb{R}$ では解をもたないが，$\mathbb{C}$ では $\pm\sqrt{-1}$ なる相異なる 2 解をもつことは周知である．この節では初等整数論をやっているのだから，

$$K=\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z},\qquad p\ \text{は任意の素数}$$

としよう．この場合でも $p=2$ と $p\neq 2$ とは事情が異なる．$p=2$ は素数には違いないが，奇素数($p\neq 2$, odd primes)と比較して，2 次の問題に対しては例外的にふるまう．2 は偶素数(even prime)であるが，それを oddest prime (最も奇なる素数)と呼ぶ人もあるくらいである．一方，

$$\mathbb{F}_2=\mathbb{Z}/2\mathbb{Z}$$

は 0 と 1 の 2 元しかないから，すべての場合を数え上げても知れている：

2 次式	x^2	x^2+x	x^2+1	x^2+x+1
解	0	0, 1	1	ナシ

以下，$p\neq 2$ と仮定する． (2) の左辺に a をかけて変形して

(3) $$0=a(ax^2+bx+c)=(ax)^2+2(ax)\frac{b}{2}+ac$$

$$=\left(ax+\frac{b}{2}\right)^2-\frac{d}{4},\qquad d=b^2-4ac\quad(\text{判別式}).$$

したがって，方程式 $ax^2+bx+c=0$ の解は：

(4)

判別式	$d=0$	$d\neq 0$，平方	$d\neq 0$，非平方
解の数	1	2	0
解	$-\dfrac{b}{2a}$	$-\dfrac{b}{2a}\pm\dfrac{\sqrt{d}}{2a}$	———

となる．これは $K=\mathbb{R}$ のとき $d=0$, $d>0$, $d<0$ に対して解の数が $1, 2, 0$ となることに対応する．

さて，(3) で $ax+b/2$ を改めて x とおき，$d/4$ を改めて a とおけば，方程式は

(5)　　$x^2=a$,　　すなわち　　$x^2\equiv a \pmod p$

となる．そこで $p\nmid a$ として(すなわち $\mathbb{F}_p$ で $a\neq 0$ として)

(6)　　$$\left(\frac{a}{p}\right)\overset{\text{def}}{=}\begin{cases} 1, & x^2\equiv a\,(p)\text{ が解をもつ,} \\ -1, & x^2\equiv a\,(p)\text{ が解をもたない}\end{cases}$$

とおく[1]．これがいわゆる**ルジャンドル‐ガウスの指標**である．記号 $\left(\frac{a}{p}\right)$ は場所を取るので，本稿では記号 $\lambda_p(a)$ を用いることにする．すなわち：

(7)　　$$\lambda_p(a)\overset{\text{def}}{=}\begin{cases} 1, & a\in(\mathbb{F}_p{}^\times)^2, \\ -1, & a\notin(\mathbb{F}_p{}^\times)^2\end{cases}$$

とあらわすことができる．指標という言葉が示すように，

命題 1　　$\lambda_p:\mathbb{F}_p{}^\times\longrightarrow\mathbb{C}^\times$

はアーベル群 $\mathbb{F}_p{}^\times$ の指標である：

$$\lambda_p\in\widehat{\mathbb{F}_p{}^\times}.$$

証明　$\mathbb{F}_p{}^\times$ は巡回群であるから r をその生成元とする[2]．

$$a=r^{\nu(a)}$$

と書くと $\nu(a)$ は mod $(p-1)$ で定まる．$p-1$ は偶数になることに注意．

(8)　　a が平方　$\Longleftrightarrow$　$\nu(a)$ が偶数

だから

(9)　　$\lambda_p(a)=(-1)^{\nu(a)}$

である．また

$$ab=r^{\nu(ab)}=r^{\nu(a)}\cdot r^{\nu(b)}=r^{\nu(a)+\nu(b)}$$

より

(10)　　$\nu(ab)\equiv\nu(a)+\nu(b)\quad(p-1)$

である．(9), (10) から

1）(p) は $(\text{mod}\ p)$ の略記．$x^2\equiv a\,(p)$ が解をもつときは2つある．また本稿では $a\in\mathbb{Z}$ と $a \bmod p\in\mathbb{F}_p$ をときどき混用する．上手な情況判断をお願いする．

2）r はいわゆる mod p の原始根である．

$$\lambda_p(ab) = (-1)^{\nu(ab)} = (-1)^{\nu(a)+\nu(b)}$$
$$= (-1)^{\nu(a)} \cdot (-1)^{\nu(b)} = \lambda_p(a) \cdot \lambda_p(b),$$

すなわち

(11) $\quad \lambda_p(ab) = \lambda_p(a) \cdot \lambda_p(b), \qquad a, b \in \mathbb{F}_p{}^{\times}$

が成り立つから λ_p は $\mathbb{F}_p{}^{\times}$ の指標になる，Q.E.D.

命題 2　λ_p は指標群 $\widehat{\mathbb{F}_p{}^{\times}}$ の中のただ 1 つの位数 2 の元である．

証明　λ_p の値が ± 1 だから

$$\lambda_p{}^2 = \varepsilon, \qquad \text{単位指標}$$

である．一方，$\mathbb{F}_p{}^{\times}$ の生成元 r に対しては

$$\lambda_p(r) = (-1)^{\nu(r)} = (-1)^1 = -1$$

となるから $\lambda_p \neq \varepsilon$ で λ_p の位数は 2 である．$\widehat{\mathbb{F}_p{}^{\times}}$ は位数 $p-1$ の巡回群だから λ_p は位数 2 のただ 1 つの指標にほかならない，Q.E.D.

命題 3　$p \nmid a$ のとき

$$\lambda_p(a) \equiv a^{(p-1)/2} \quad (p)$$

である．

証明　(9) により

(12) $\quad (-1)^{\nu(a)} \equiv a^{(p-1)/2} \quad (p)$

をいえばよい．$\mathbb{F}_p{}^{\times}$ は位数 $p-1$ の巡回群で r はその生成元だから

(13) $\quad r^{p-1} = 1, \qquad$ すなわち $\qquad r^{p-1} \equiv 1 \quad (p).$[3)]

$p-1$ は偶数だから

$$r^{p-1} = (r^{(p-1)/2})^2 = 1.$$

したがって，

(14) $\quad r^{(p-1)/2} = \pm 1.$

r は位数 $p-1$ であるから (14) で $+1$ は起こらない．よって

(15) $\quad r^{(p-1)/2} = -1, \qquad$ すなわち $\qquad r^{(p-1)/2} \equiv -1 \quad (p).$

任意の a について，$a = r^{\nu(a)}$ が $\nu(a)$ の定義であったから，(15) の両辺を $\nu(a)$ 乗して

$$(-1)^{\nu(a)} = (r^{(p-1)/2})^{\nu(a)} = (r^{\nu(a)})^{(p-1)/2} = a^{(p-1)/2}.$$

3）(13) はいうまでもなく，フェルマ - オイラーの定理である．

これは (12) にほかならない，Q.E.D.

定理 1 (第 1 補充法則)　$p \neq 2$ のとき $$\lambda_p(-1) = (-1)^{(p-1)/2}.$$

証明　命題 3 で $a = -1$ とおくと

$$\lambda_p(-1) \equiv (-1)^{(p-1)/2} \quad (p).$$

両辺の値が ± 1 で，p は奇数だから等号になる，Q.E.D.

注意 1　定理 1 は，$p \neq 2$ のとき，

(16)　　$x^2 \equiv -1\ (p)$ が解をもつ　$\Longleftrightarrow$　$p \equiv 1 \quad (4)$

と同じことである．

これは若年のガウスが ‘たいそう美しいと思った驚くべき算術的真理’ である[4]．われわれは実質的に $\mathbb{F}_p^\times$ が巡回群であること (すなわち原始根の存在) だけを用いて 3 つの命題を証明し，(16) をスルスルと出してしまったので，あまり美しいと思う余裕がなかった．これは私の責任であってまことに申しわけなく思う．(注意終)

さて，第 1 があれば当然第 2 がなければならぬ．

定理 2 (第 2 補充法則)　$p \neq 2$ のとき $$\lambda_p(2) = (-1)^{(p^2-1)/8}.$$

注意 2　定理 2 は，$p \neq 2$ のとき，

(17)　　$x^2 \equiv 2\ (p)$ が解をもつ　$\Longleftrightarrow$　$p \equiv \pm 1 \quad (8)$

と同じことである．

定理 2 の証明には少しばかり代数的整数のことが必要になる．証明は抜きにして，用いる事実を書いておく[5]．

4）　前回 § 2 の《Disquisitiones arithmeticae》に関する記事参照．

5）　証明はたいていの代数的整数論の教科書参照．たとえば高木貞治『代数的整数論』(岩波書店，1971) の最初の数ページで十分．

定義 1　複素数 $\alpha \in \mathbb{C}$ が**代数的整数**(algebraic integer)であるとは，ある多項式

$$f(X) = X^n + a_1 X^{n-1} + \cdots + a_n, \qquad a_i \in \mathbb{Z}, \quad n \geqq 1$$

があって

$$f(\alpha) = 0$$

となることである．

代数的整数の全体を $\bar{\mathbb{Z}}$ と書く．

命題 4　$\bar{\mathbb{Z}}$ は $\mathbb{C}$ の部分環になる．

$$\bar{\mathbb{Z}} \cap \mathbb{Q} = \mathbb{Z}$$

である．

定義 2 (合同概念の $\bar{\mathbb{Z}}$ への拡張)　$\bar{\mathbb{Z}}$ の元 $\mu \neq 0$ を用いて，$\alpha, \beta \in \bar{\mathbb{Z}}$ に対して

$$(18) \qquad \alpha \equiv \beta \quad (\mu) \quad \overset{\text{def}}{\Longleftrightarrow} \quad \mu \mid \alpha - \beta$$

により mod μ の合同を定義する[6)]．

命題 5　p を素数とすると，$\alpha, \beta \in \bar{\mathbb{Z}}$ に対して

$$(\alpha+\beta)^p \equiv \alpha^p + \beta^p \quad (p)$$

が成り立つ．

定理 2 の証明　$\zeta = e^{2\pi i/8}$ とおく．

$$\zeta^4 = -1$$

だから

$$\zeta^2 + \zeta^{-2} = 0.$$

いま $\eta = \zeta + \zeta^{-1}$ とおくと

$$\eta^2 = (\zeta + \zeta^{-1})^2 = \zeta^2 + 2 + \zeta^{-2} = 2.$$

明らかに ζ, η は代数的整数：$\zeta, \eta \in \bar{\mathbb{Z}}$.

命題 3 で $a = 2$ とおくと，

$$\eta^{p-1} = (\eta^2)^{(p-1)/2} = 2^{(p-1)/2} \equiv \lambda_p(2) \quad (p).$$

---

6)　$\mu | \alpha - \beta$ は $\alpha - \beta = \mu\gamma, \gamma \in \bar{\mathbb{Z}}$ のことである．定義 2 でとくに α, β, μ がすべて $\mathbb{Z}$ の元であれば，(18) の合同関係は $\mathbb{Z}$ における従来のそれと一致する．

したがって，

(19)　$\lambda_p(2)\eta \equiv \eta^p = (\zeta+\zeta^{-1})^p \equiv \zeta^p+\zeta^{-p} \quad (p)$　（命題5より）.

さて

$$p \equiv \pm 1 \quad (8) \implies \zeta^p+\zeta^{-p} = \zeta+\zeta^{-1} = \eta,$$
$$p \equiv \pm 3 \quad (8) \implies \zeta^p+\zeta^{-p} = \zeta^3+\zeta^{-3} = -\zeta^{-1}-\zeta = -\eta.$$

したがって

(20)　$$\zeta^p+\zeta^{-p} = \begin{cases} \eta, & p \equiv \pm 1 \quad (8), \\ -\eta, & p \equiv \pm 3 \quad (8). \end{cases}$$

そこで，

$$\omega = \frac{p^2-1}{8}$$

とおけば，(19), (20) より

(21)　$(-1)^\omega \eta = \zeta^p+\zeta^{-p} \equiv \lambda_p(2)\eta \quad (p).$

この両辺に η をかけて，$\eta^2 = 2$ を用いると

$$(-1)^\omega \cdot 2 \equiv \lambda_p(2) \cdot 2 \quad (p).$$

$p \neq 2$ だから

$$(-1)^\omega \equiv \lambda_p(2) \quad (p).$$

この両辺の値が ±1 だから等号が成り立つ，Q.E.D.

---

§5．ガウスの相互律

---

p, q を相異なる奇素数とする．

$$p^* = (-1)^{(p-1)/2} p$$

とおく．

定理 1 (ガウスの相互律)

$$\lambda_p(q) = \lambda_q(p^*).$$

注意 1　これは文句なしに美しい．いろいろの証明法があるが，ここでは λ_p が群 $\mathbb{F}_p{}^\times$ の指標であることを十分に用いたガウスの和による証明を与える．(注意終)

念のため，前回 §3 の定義 1 を復習すると：

定義 1　p を素数，$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$，$\zeta = e^{2\pi i/p}$ とする．$\xi \in \mathbb{F}_p$，$\chi \in \widehat{\mathbb{F}_p{}^\times}$ に対して

$$\tau_\xi(\chi) \overset{\text{def}}{=} \sum_{x \in \mathbf{F}_p{}^\times} \chi(x)\zeta^{\xi x}$$

とおき，ξ, χ に関する**ガウスの和**とよぶ．

とくに，$\tau_1(\chi) = \tau(\chi)$ とおく：

$$\tau(\chi) \overset{\text{def}}{=} \sum_{x \in \mathbf{F}_p{}^\times} \chi(x)\zeta^{x}.$$

命題 1　$\xi \neq 0 \implies \tau_\xi(\chi) = \bar{\chi}(\xi)\tau(\chi).$

証明　$\chi(\xi)\tau_\xi(\chi) = \chi(\xi)\sum_x \chi(x)\zeta^{\xi x}$

$$= \sum_x \chi(\xi x)\zeta^{\xi x} = \tau(\chi), \qquad \text{Q.E.D.}$$

命題 2　$p \neq 2,\ \chi \neq \varepsilon \implies \tau(\chi)\tau(\bar{\chi}) = \chi(-1)p.$

とくに $\chi = \lambda_p$ として

$$\tau(\lambda_p)^2 = p^* \qquad (\text{§ 4 定理 1 より}).$$

証明　$S = \sum_{\xi \in \mathbf{F}_p{}^\times} |\tau_\xi(\chi)|^2 = \sum_\xi \tau_\xi(\chi)\overline{\tau_\xi(\chi)}$

を 2 通りの方法で計算する．まず，命題 1 から

$$(1) \qquad S = \sum_\xi \bar{\chi}(\xi)\tau(\chi)\chi(\xi)\overline{\tau(\chi)} = (p-1)|\tau(\chi)|^2.$$

次に

$$\tau_\xi(\chi)\overline{\tau_\xi(\chi)} = \sum_x \chi(x)\zeta^{\xi x} \sum_y \bar{\chi}(y)\zeta^{-\xi y} = \sum_{x,y} \chi(xy^{-1})\zeta^{\xi(x-y)}.$$

したがって，

(2) $$S = \sum_{x,y} \chi(xy^{-1}) \sum_{\xi \in \mathbf{F}_p{}^\times} \zeta^{\xi(x-y)}$$

$$= \sum_{x,y} \chi(xy^{-1})((\sum_{\xi \in \mathbf{F}_p} \zeta^{\xi(x-y)})-1).$$

ここで

$$\xi \longmapsto \zeta^{\xi(x-y)}$$

は群 $\mathbf{F}_p{}^+$ の指標だから

(3) $$\sum_{\xi \in \mathbf{F}_p} \zeta^{\xi(x-y)} = \begin{cases} p, & x = y, \\ 0, & x \neq y. \end{cases}$$

$\chi \neq \varepsilon$ だから，

$$\sum_{x,y} \chi(xy^{-1}) = (\sum_x \chi(x))(\sum_y \bar{\chi}(y)) = 0$$

に注意して (3) を (2) に代入すれば，

(4) $$S = p \sum_x \chi(1) = p(p-1).$$

(1) と (4) から S を消去して $p-1$ で割れば

(5) $$|\tau(\chi)|^2 = p.$$

さて，

$$\overline{\tau(\chi)} = \sum_x \overline{\chi(x)}\,\zeta^{-x} = \sum_x \overline{\chi(-x)}\,\zeta^x$$

$$= \chi(-1) \sum_x \bar{\chi}(x)\zeta^x = \chi(-1)\tau(\bar{\chi})$$

だから (5) から命題が証明される．$\chi = \lambda_p$ のときは $\bar{\chi} = \chi$ で §4 の定理 1 (第 1 補充法則) から

$$\chi(-1)p = p^*, \qquad \text{Q.E.D.}$$

定理 1 の証明　まず,

(6)　$$\tau(\lambda_p)^{q-1} = (\tau(\lambda_p)^2)^{(q-1)/2} = p^{*(q-1)/2} \equiv \lambda_q(p^*) \quad (q).$$

第 2 の等号は命題 2 に, 最後の合同式は § 4 の命題 3 による. この (6) の両辺に $\tau(\lambda_p)$ をかけて

(7)　$$\tau(\lambda_p)^q \equiv \lambda_q(p^*)\tau(\lambda_p) \quad (q).$$

一方,

$$\tau(\lambda_p) \overset{\text{def}}{=} \sum_{x \in \mathbf{F}_p^\times} \lambda_p(x)\zeta^x$$

から

(8)　$$\tau(\lambda_p)^q \equiv \sum_x \lambda_p(x)^q \zeta^{qx} = \sum_x \lambda_p(x)\zeta^{qx} = \tau_q(\lambda_p) \quad (q).$$

最初の合同式は § 4 の命題 5, 最後の等号は § 3 の定義 1 による. (7), (8) から

(9)　$$\lambda_p(q)\tau(\lambda_p) = \tau_q(\lambda_p) \equiv \lambda_q(p^*)\tau(\lambda_p) \quad (q).$$

最初の等号は命題 1 による.

そこで, (9) の両辺に $\tau(\lambda_p)$ をかけて命題 2 を用いると

(10)　$$\lambda_p(q)p^* \equiv \lambda_q(p^*)p^* \quad (q).$$

この両辺を p^* で約して

(11)　$$\lambda_p(q) \equiv \lambda_q(p^*) \quad (q).$$

ここで, (11) の両辺の値が ± 1 なることに注意すれば,

(12)　$$\lambda_p(q) = \lambda_q(p^*)$$

を得る, Q.E.D.

注意 2　目がクルクルまわるようでしょう. 数学に証明はたくさんありますが, これほど不思議な気持に襲われる証明はめったにないと思います. (注意終)

さて,

$$\lambda_p(a) = \left(\frac{a}{p}\right)$$

と, ルジャンドル - ガウスの記号にもどすと, いうまでもなく次の 3 式が証明できたことになる. 以下 p, q は相異なる奇素数である.

I（第1補充法則）　$\left(\frac{-1}{p}\right)=(-1)^{(p-1)/2}$,

II（第2補充法則）　$\left(\frac{2}{p}\right)=(-1)^{(p^2-1)/8}$,

III（ガウスの相互律）　$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\{(p-1)/2\}\cdot\{(q-1)/2\}}$.

相互律はいうまでもなく

$$x^2\equiv a \quad (p)$$

に解があるかどうかを決定するのに役立つ．しかし，相互律の真の合理化は初等整数論すなわち $\mathbb{Z}$ ないし $\mathbb{Q}$(有理数体)の整数論ではなく，$\bar{\mathbb{Z}}$ ないし $\bar{\mathbb{Q}}$($\mathbb{Q}$ の代数的閉体)における整数論(代数的整数論)を展開することによってなされる．このことは定理3の証明に用いられたガウスの和が1の原始 p 乗根 $\zeta=e^{2\pi i/p}$ を含んでいることから推察される．命題2は2次体 $\mathbb{Q}(\sqrt{p^*})$ が円分体 $\mathbb{Q}(\zeta)$ の部分体になることを示す．

そして

(13)　　$\lambda_q(p^*)=1 \iff q$ が $\mathbb{Q}(\sqrt{p^*})/\mathbb{Q}$ で完全分解する

が成り立つ．(13) は，次の (14) と同値になる．

(14)　　$\lambda_p(q)=1 \iff \lambda_q(p^*)=1.$

(14) は相互律にほかならないから，(13) は1つの相互律の合理化である．ガウスの相互律を任意の相対アーベル体 K/k に (13) の方向に拡張したものが類体論における**アルティンの相互律**である[7]．

§6．正17角形の作図

「1796年3月30日の朝，十九歳の青年ガウスが目ざめて臥床から起き出

7）　これらの事情の詳細については拙著『数論序説』(裳華房)を参照．

でようとする刹那に正十七角形の作図法に思い付いた．……」[8)]

いうまでもなく高木貞治先生『近世数学史談』(岩波文庫，1995)の第1話「正十七角形のセンセーション」の書き出しである．本節ではこの作図問題を**ガウスの和**(および後で定義する**ヤコビの和**)を用いて解いてみよう．

まず，作図という幾何学の言葉を代数学の言葉に直すことについて注意する．紙と鉛筆と定木(目盛のないもの，目盛があっても使わなければよい)とコンパスを用意する．紙に2点をとり片方を0，片方を1とよぶ．0と1を定木で結ぶ；x 軸ができる．次に1を中心として -1 を通る円，-1 を中心として1を通る円を描いて交点を結べば y 軸ができる．0を中心として1を通る円と y 軸との交わりとして $i=\sqrt{-1}$ が定まる．これで座標の入った平面すなわち複素平面 $\mathbb{C}$ が得られた．$\{0,1\}$ から出発して四則は作図可能である．したがって，有理数体 $\mathbb{Q}$ はすでに作図された点集合と考える．

いま $\mathbb{C}$ と $\mathbb{Q}$ の任意の中間体 K をとる．K の元は平面の点でもある．$a, b \in K$ に対して a と b を結ぶ直線，a を中心とし b を通る円が得られる．これらを K 線，K 円という(図3〜図5)．K 線と K 線，K 線と K 円，K 円と K 円の交点として $\mathbb{C}$ の点ができるが，これらの点は K の高々2次拡大 K^* に入る：

$$[K^*:K] \leqq 2.$$

複素数 $\alpha \in \mathbb{C}$ が**作図可能**であるとは，$\{0,1\}$ から，したがって $\mathbb{Q}$ から有限個の $\mathbb{Q}$ 線，$\mathbb{Q}$ 円を作り，それらの交点として K_1 点，

$$[K_1:\mathbb{Q}] \leqq 2$$

を得，K_1 点を用いて有限個の K_1 線，K_1 円を作り，それらの交点として K_2 点，

$$[K_2:K_1] \leqq 2$$

を得，……とつづけて，α がある K_n に入るようにできることである．このようにして次の定義を得る．

8）『岩波数学辞典(第4版)』(岩波書店，2007)によれば，Carl Friedrich Gauss, 1777.4.30−1855.2.23であるから，1796年3月30日にはまだ18歳であった．

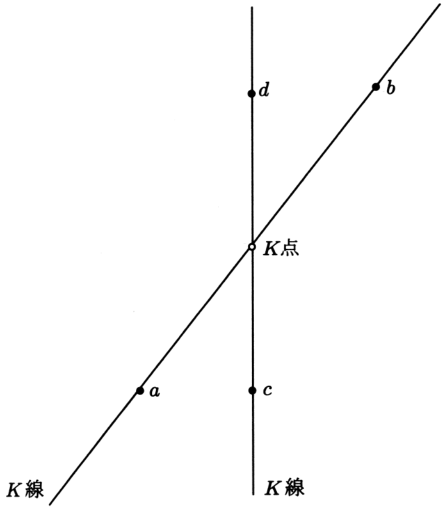


図3

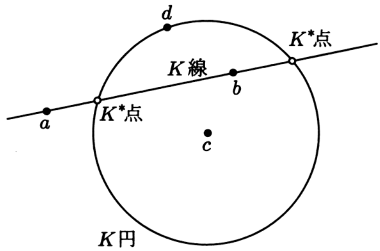


図4

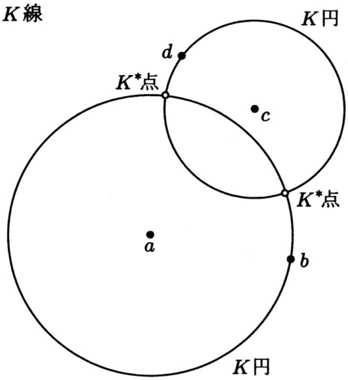


図5

定義1　$\alpha \in \mathbb{C}$ が次の条件を満足するとき**作図可能**であるという；$\mathbb{C}$ の部分体の列

$$\mathbb{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots\cdots \subset K_n$$

で,

$$\alpha \in K_n, \qquad [K_i : K_{i-1}] \leqq 2, \qquad 1 \leqq i \leqq n$$

なるものが存在する.

以下, $k \in \mathbb{N} = \{1, 2, 3, \cdots\}$ に対し

$$\zeta_k = e^{2\pi i/k}$$

とおく．

命題 1　ζ_{2^k}, $k \in \mathbb{N}$, は作図可能である．

証明　k についての帰納法．$k=1$ なら $\zeta_2 = -1 \in \mathbb{Q}$ だから作図可能である．

次に，ζ_{2^k} が作図可能であるとすると

$$(\zeta_{2^{k+1}})^2 = \zeta_{2^k}$$

だから，$\zeta_{2^k} \in K_n$ (定義 1 で $\alpha = \zeta_{2^k}$ とおけ) とすると

$$\zeta_{2^{k+1}} \in K_{n+1} = K_n(\sqrt{\zeta_{2^k}})$$

となり，$\zeta_{2^{k+1}}$ も作図可能になる，Q.E.D.

問題が代数化されたから，次にヤコビの和を導入する．以下，$\chi \in \widehat{\mathbb{F}_p^\times}$ に対して $\chi(0)=0$ とおいて χ を $\mathbb{F}_p$ 上の関数と考える．

定義 2　$p \neq 2$, $\chi, \psi \in \widehat{\mathbb{F}_p^\times}$, $\chi \neq \varepsilon$, $\psi \neq \varepsilon$ に対して

$$J(\chi, \psi) \stackrel{\text{def}}{=} \sum_{x+y=1} \chi(x)\psi(y)$$

のことを**ヤコビの和**という．

命題 2　$\chi, \psi, \chi\psi$ の 3 つとも $\neq \varepsilon$ ならば

$$J(\chi, \psi) = \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)}\text{[9]}.$$

証明　$\tau(\chi)\tau(\psi) = (\sum_x \chi(x)\zeta^x)(\sum_y \psi(y)\zeta^y)$

$$= \sum_{x,y} \chi(x)\psi(y)\zeta^{x+y} = \sum_t (\sum_{x+y=t} \chi(x)\psi(y))\zeta^t.$$

ここで，もし $t=0$ ならば

$$\sum_{x+y=0} \chi(x)\psi(y) = \sum_x \chi(x)\psi(-x) = \psi(-1)\sum_x (\chi\psi)(x) = 0$$

9)　$\chi\psi \neq \varepsilon$ だから §5 の命題 2 より $\tau(\chi\psi) \neq 0$ に注意．

($\chi\psi \neq \varepsilon$ を用いた)．また，$t \neq 0$ ならば，

$$x = tu, \qquad y = tv$$

と書くと $x+y=t$ のとき $u+v=1$ で

$$\sum_{x+y=t} \chi(x)\psi(y) = (\chi\psi)(t) \sum_{u+v=1} \chi(u)\psi(v) = (\chi\psi)(t)J(\chi, \psi).$$

したがって，

$$\tau(\chi)\tau(\psi) = \sum_{t \in \mathbb{F}_p^\times} (\chi\psi)(t)J(\chi, \psi)\zeta^t$$
$$= J(\chi, \psi)\tau(\chi\psi), \qquad \text{Q.E.D.}$$

注意 1　体 $\mathbb{F}_p$ についてのガウスの和，ヤコビの和がそれぞれ体 $\mathbb{R}$ についてのガンマ関数，ベータ関数とよく似ていると思いませんか？

→	$\mathbb{R}$	$\mathbb{F}_p$
↓	$\Gamma(s) = \int_0^\infty x^s e^{-x} \frac{dx}{x}$	$\tau(\chi) = \sum_x \chi(x)\zeta^x$
2変数化	$B(p, q) = \frac{\Gamma(p)\Gamma(q)}{\Gamma(p+q)}$	$J(\chi, \psi) = \frac{\tau(\chi)\tau(\psi)}{\tau(\chi\psi)}$

命題 3　$m \geqq 3,\ p \equiv 1\ (m)$，指標 $\chi \in \widehat{\mathbb{F}_p^\times}$ の位数を m とすれば

$$\tau(\chi)^m = \chi(-1)pJ(\chi, \chi)J(\chi, \chi^2)\cdots\cdots J(\chi, \chi^{m-2}).$$

証明　$\chi \neq \varepsilon,\ \chi^2 \neq \varepsilon$ だから命題 2 から

(1)　$$\tau(\chi)^2 = J(\chi, \chi)\tau(\chi^2).$$

両辺に $\tau(\chi)$ をかけて同様にして

(2)　$$\tau(\chi)^3 = J(\chi, \chi)\tau(\chi)\tau(\chi^2) = J(\chi, \chi)J(\chi, \chi^2)\tau(\chi^3).$$

このように続けて

(3)　$$\tau(\chi)^{m-1} = J(\chi, \chi)J(\chi, \chi^2)\cdots\cdots J(\chi, \chi^{m-2})\tau(\chi^{m-1})$$

となるが，

$$\chi^{m-1} = \chi^{-1} = \bar{\chi}$$

で

$$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p \qquad (\S 5 \text{ 命題 } 2 \text{ より})$$

だから，(3) の両辺に $\tau(\chi)$ をかけて，Q.E.D.

定義 3　$n \geqq 0$ に対して

$$F_n = 2^{2^n}+1$$

とおく[10]．これは**フェルマの数**とよばれる．フェルマの数になる素数を**フェルマの素数**という．

注意 2　$F_0 = 3,\quad F_1 = 5,\quad F_2 = 17,\quad F_3 = 257,\quad F_4 = 65537$

は素数であるが，

$$F_5 = 4294967297$$

は素数でない．フェルマは F_n がみな素数であろうと推測していたが，オイラーが

$$F_5 = =641\times 6700417$$

という素因数分解を与えた．フェルマの素数が無数にあるかどうかは，まだわかっていない．

次の定理はガウスによるもので《Disquisitiones arithmeticae》の最終章(円周等分論)にある．$17 = F_2$ の場合が 1796 年 3 月 30 日の朝のハプニングであった．

> **定理 1**　$p \neq 2$ を素数，$\zeta_p = e^{2\pi i/p}$ とする．このとき，
>
> ζ_p が作図可能　$\Longleftrightarrow$　p がフェルマの素数．

証明　($\Longrightarrow$)　ζ_p が作図可能ならば定義 1 の 2 次拡大の列の最後の体 K_n に ζ_p が入る．$[K_n : \mathbf{Q}]$ は 2 の巾(ベキ)で

$$[\mathbf{Q}(\zeta_p) : \mathbf{Q}] \mid [K_n : \mathbf{Q}]$$

だから

$$[\mathbf{Q}(\zeta_p) : \mathbf{Q}] = \varphi(p) = p-1$$

が 2 の巾で，したがって，$p = 1+2^k$．ここで k が奇数因数を含めば p は素数でなくなるから

$$p = 1+2^{2^n} = F_n \quad ; \quad \text{フェルマの素数}$$

10)　$2^{2^n} = 2^{(2^n)}$．これはもちろん $(2^2)^n = 4^n$ とはちがう ($n = 3$ とせよ)．

でなければならない．

(⟸)　この方が重要である(‘正17角形は作図可能である’ はこの方に属する)．まず，ζ_p の作図可能性をガウスの和の作図可能性に還元する．実際，$\chi \in \widehat{\mathbf{F}_p{}^\times}$ に対して

$$\tau(\chi) = \sum_{x \in \mathbf{F}_p{}^\times} \chi(x)\zeta_p{}^x$$

で，これをすべての指数 χ について加えると

$$(4) \qquad \sum_\chi \tau(\chi) = \sum_\chi \sum_x \chi(x)\zeta_p{}^x = \sum_x \Big(\sum_\chi \chi(x)\Big)\zeta_p{}^x.$$

ここで

$$\sum_\chi \chi(x) = \begin{cases} p-1, & x=1, \\ 0, & x \neq 1. \end{cases}$$ [11)]

したがって (4) から

$$(5) \qquad \sum_\chi \tau(\chi) = (p-1)\zeta_p.$$

つまり，各 $\tau(\chi)$ が作図可能ならば ζ_p が作図可能になる．したがって各 $\tau(\chi)$ が作図可能なことをいうのであるが，まず $\chi = \varepsilon$ と $\chi = \lambda_p$ については

$$\tau(\varepsilon) = \sum_x \zeta^x = -1 \in \mathbf{Q},$$

$$\tau(\lambda_p)^2 = p^* \qquad (\text{§ 5 命題 2}),$$

すなわち

$$\tau(\lambda_p) \in \mathbf{Q}(\sqrt{p^*})$$

だから問題はない．以下，$\chi \neq \varepsilon, \lambda_p$ と仮定する．p はフェルマの素数と仮定するのだから

$$p = 2^k + 1$$

の形である．$\widehat{\mathbf{F}_p{}^\times}$ は位数 $p-1$ の巡回群だから各 χ の位数 $m = 2^r$ で，χ の仮定から $m \geqq 3$ である．$r \leqq k$ だから $p \equiv 1\,(m)$ である．したがって，命題3

---

11)　ここでは $G = \mathbf{F}_p{}^\times$ とするとき $\widehat{G}$ の上の和 $\sum_\chi$ がとられているが，G の双対性：$\widehat{\widehat{G}} = G$ により G を $\widehat{G}$ の指標群と考えることができて以前の公式(§ 3(7)) が使える．

から

(6) $$\tau(\chi)^m = \chi(-1)pJ(\chi,\chi)J(\chi,\chi^2)\cdots\cdots J(\chi,\chi^{m-2}).$$

ここで，$J(\chi,\chi^j)$ は乗法的指標しか定義に用いていないから

$$J(\chi,\chi^j) \in \mathbb{Q}(\zeta_{p-1}) = \mathbb{Q}(\zeta_{2^k})$$

で，命題1により $J(\chi,\chi^j)$ は作図可能になる．(6) から

$$\tau(\chi)^m = \tau(\chi)^{2^r}$$

は作図可能になる．これは2の巾だから $\tau(\chi)$ も作図可能になる，Q.E.D.

ちょっと紙数の余裕がありますので，F_5 が素数でないことを見るオイラーの方法を紹介しましょう．まず少し一般的に，

命題 $a \in \mathbb{N}$ (自然数)，$p \neq 2$，奇素数，$n \in \mathbb{N}$，とする．

$$p \mid a^{2^n}+1 \implies 2^{n+1} \mid p-1.$$

証明 仮定から($\mathbb{F}_p$ で考えて)，

$$a^{2^n} = -1,$$

したがって

$$a^{2^{n+1}} = 1.$$

a の $\mathbb{F}_p^\times$ での位数は 2^k，$0 \leqq k \leqq n+1$．もし $k \leqq n$ とすると

$$a^{2^n} = 1$$

となり，$-1=1$ で $p \neq 2$ に矛盾する．よって

$$k = n+1.$$

一方，$a^{p-1}=1$．よって

$$2^{n+1} \mid p-1, \qquad \text{Q.E.D.}$$

さて，上の命題で $a=2$，$n=5$ とする．

$$F_5 = 2^{2^5}+1 = 2^{32}+1$$

である．したがって

$$p \mid F_5 \implies 2^6 \mid p-1, \qquad \text{すなわち，} p = 1+k\cdot 2^6.$$

k に1から10まで入れて表を作る：

k	1	2	3	4	5	6	7	8	9	10
$1+k\cdot 2^6$	65	129	193	257	321	385	449	513	577	641
素数？	No	No	Yes	Yes	No	No	Yes	No	Yes	Yes

この素数 193，257，449，577，641 の中から

$$F_5 = 4294967297$$

を割るものを探すと 641 に行き当たる．

$$F_5 = 641 \times 6700417$$

となる．ついでながら 6700417 が素数であることが次のようにしてわかる．

$$p \mid 6700417$$

ならば $p \mid F_5$ だから

$$p \equiv 1 \quad (2^6)$$

が出る．したがってこのような形の素数で

$$\sqrt{6700417} = 2588.516\cdots$$

より小さいものがどれも 6700417 を割らないことを見ればよい．このような素数は次の 11 個である：

193，257，449，577，641，769，1153，1217，1409，
1601，2113．

これらがどれも 6700417 を割らないことは容易に確かめられる．お急ぎの方は電卓を使うと早くすみます．

第3回

ガウスの和の符号
調和多項式

「この平方根の符号の決定には全く悩まされた．何もかもいやになったほどだ．ここ4年来，これの解決のための幾多の空しい試みで毎週が過ぎて行った．ところが，2, 3日前に証明がうまくいったのだ．それは自分自身の努力というよりは，むしろ神の恩寵によって，雷に打たれたように一瞬にして多年の謎が解けたのだ．」

これは28歳のガウスが1805年9月3日に友人のW. Olbersに宛てた手紙の一部分(の拙訳)である．今回はこのガウスの結果の，本質的にシュアー(I. Schur)による証明を学ぶことにしたい．最短の証明ではないが，mod p のフーリエ解析の醍醐味を味わえる．

§7．ガウスの和の符号

奇素数 p に関するルジャンドル - ガウスの指標を λ_p とし，$\tau(\lambda_p)$ をそのガウスの和とする：

$$(1)\qquad \tau(\lambda_p) = \sum_{x \in \mathbf{F}_p^\times} \lambda_p(x)\zeta^x, \qquad \zeta = e^{2\pi i/p}.$$

前回の§5，命題2によれば，

(2) $$\tau(\lambda_p)^2 = p^*, \qquad p^* = (-1)^{(p-1)/2}p$$

である．いい換えれば，

(3) $$\tau(\lambda_p) = \begin{cases} \pm\sqrt{p}, & p \equiv 1 \quad (4), \\ \pm i\sqrt{p}, & p \equiv 3 \quad (4). \end{cases}$$

ガウスの日記(1801年5月)によれば，ガウスは (3) でいずれも＋の方が成り立つと予想していたが，その証明に成功したのは1805年8月30日のことであった．上に引用した手紙にあるように，プラスかマイナスかが4年間も決まらなければ，さぞいらいらしたことであろう．

我々の目標とする定理を再記すると：

定理 (ガウス)

$$\tau(\lambda_p) = \begin{cases} \sqrt{p}, & p \equiv 1 \quad (4), \\ i\sqrt{p}, & p \equiv 3 \quad (4). \end{cases}$$

証明の基礎になる一般的事実は，§3の**定理2**である．すなわち，G を位数 N の有限アーベル群，$L(G)$ を $\mathbb{C}$ に値をもつ G 上の関数の全体，$\langle\ ,\ \rangle$ を

(4) $$\langle f, g\rangle = \frac{1}{N}\sum_{x\in G} f(x)\bar{g}(x), \qquad f, g \in L(G)$$

で定まる $L(G)$ の内積とすると，G の指標群 $\widehat{G} \subset L(G)$ が N 次元のヒルベルト空間 $(L(G), \langle\ ,\ \rangle)$ の正規直交底をなす，という定理である．

とくに，

$$G = \mathbb{F}_p{}^+ \qquad (\text{有限体 } \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \text{ の加法群，} p \text{ は奇素数})$$

とすると，§3で見たように(§3の (12) 参照)

(5) $$\widehat{G} = \{\,\psi_\xi\,;\,\psi_\xi(x) = \zeta^{\xi x}, \zeta = e^{2\pi i/p}, x, \xi \in \mathbb{F}_p\}$$

によって指標群が記述される．しばらく体 $\mathbb{F}_p$ の加法のみを考えて，$f \in L(\mathbb{F}_p)$ に対して

(6) $$(Tf)(\xi) \overset{\text{def}}{=} \sum_{x\in\mathbb{F}_p} f(x)\psi_\xi(x), \qquad \xi \in \mathbb{F}_p$$

とおく[1]．$Tf \in L(\mathbb{F}_p)$ で，$f \longmapsto Tf$ はベクトル空間 $L(\mathbb{F}_p)$ の1次変換にな

る．(6) の右辺で

$$\psi_\xi(x) = \zeta^{\xi x} = \psi_x(\xi)$$

に注意すれば，(6) の両辺の変数 ξ を消去して (6) を

$$(6)^* \qquad Tf = \sum_{x \in \mathbb{F}_p} f(x)\psi_x$$

とも書くことができる．ヒルベルト空間にはユニタリ変換すなわち内積を保存する 1 次変換がつきものであるが，これに関して，

命題 1 $p^{-1/2}T$ はヒルベルト空間 $L(\mathbb{F}_p)$ のユニタリ変換になる．

証明 $U = p^{-1/2}T$ がユニタリ変換とは，

$$\langle Uf, Ug \rangle = \langle f, g \rangle$$

がすべての $f, g \in L(\mathbb{F}_p)$ に対して成り立つことであるから，T についていえば

$$(7) \qquad \langle Tf, Tg \rangle = p\langle f, g \rangle, \qquad f, g \in L(\mathbb{F}_p)$$

を確かめればよい．実際 (6)* から

$$\langle Tf, Tg \rangle = \sum_{x,y} f(x)\bar{g}(y)\langle \psi_x, \psi_y \rangle \ ^{2)}$$

$$= \sum_x f(x)\bar{g}(x) = p\langle f, g \rangle, \qquad \text{Q.E.D.}$$

一般に $L(\mathbb{F}_p)$ の 1 次変換 S の随伴(adjoint) S^* は関係

$$(8) \qquad \langle Sf, g \rangle = \langle f, S^*g \rangle, \qquad f, g \in L(\mathbb{F}_p)$$

によって定義される．これを用いれば，

$$(9) \qquad S \text{ がユニタリ変換} \iff SS^* = S^*S = 1 \ ^{3)}$$

となり，(6) の T は命題 1 により

$$(10) \qquad TT^* = T^*T = p \ ^{4)}$$

1） 集合としては $\mathbb{F}_p{}^+ = \mathbb{F}_p$ であり，$L(\mathbb{F}_p{}^+)$ の定義には $\mathbb{F}_p$ の加法群の構造は反映していないから，以下 $L(\mathbb{F}_p{}^+) = L(\mathbb{F}_p)$ と書く．

2） ここで $\{\psi_x\}$ が $L(\mathbb{F}_p)$ の正規直交底であることを用いた．

3） この 1 は $L(\mathbb{F}_p) \longrightarrow L(\mathbb{F}_p)$ の恒等写像 $f \longmapsto f$ を意味する．

4） この p は $L(\mathbb{F}_p) \longrightarrow L(\mathbb{F}_p)$ の写像 $f \longmapsto pf$ を意味する．

を満足する．シュアーの方法の要点は行列式 $\det T$ の値を2つの方法で定めることである．まず，やさしい命題(命題2, 3, 4)からはじめよう．

命題2　$(T^*f)(\xi)=(Tf)(-\xi), \qquad \xi\in\mathbb{F}_p.$

証明　(6)* で f に $T^{-1}f$ を代入すると

$$f=\sum_x (T^{-1}f)(x)\psi_x$$

となるから，$\{\psi_x\}$ が正規直交底であることから

$$\text{(11)}\qquad \langle f,\psi_\xi\rangle=\sum_x (T^{-1}f)(x)\langle\psi_x,\psi_\xi\rangle=(T^{-1}f)(\xi)$$
$$=p^{-1}(T^*f)(\xi).$$

ここで最後の等式は (10) による．一方，

$$\text{(12)}\qquad \langle f,\psi_\xi\rangle=p^{-1}\sum_x f(x)\overline{\psi}_\xi(x)=p^{-1}\sum_x f(x)\psi_\xi(-x)$$
$$=p^{-1}\sum_x f(x)\psi_x(-\xi)=p^{-1}(Tf)(-\xi).$$

(11), (12) の最終項どうしを比較して，Q.E.D.

命題3　$(T^2f)(\xi)=pf(-\xi).$

証明　命題2と (10) より

$$(T^2f)(\xi)=(T^*Tf)(-\xi)=pf(-\xi), \qquad \text{Q.E.D.}$$

命題4　$T^4=p^2.$

したがって

$$(\det T)^4=p^{2p}.$$

証明　命題3から

$$(T^4f)(\xi)=(T^2\cdot T^2f)(\xi)=pT^2f(-\xi)$$
$$=p^2f(\xi), \qquad \text{Q.E.D.}$$

命題4より

$$\det T=(1\text{ の }4\text{ 乗根})\times p^{p/2}$$

となるが，この1の4乗根を正確に定めるのが第1のステップである．答は次

の命題である．

命題 5　$\det T = i^{p(p-1)/2}p^{p/2}$.

証明　f_x を $x \in \mathbb{F}_p{}^+$ の特性関数とし，$L(\mathbb{F}_p)$ の底 $\{f_x\}$ によって T に対応する行列 A の $\det A$ を求めよう：

$$(\cdots, Tf_x, \cdots) = (\cdots, f_y, \cdots)A.$$

ここで $p \times p$ 行列 $A = (a_{yx})$, $a_{yx} \in \mathbb{C}$, は関係

$$Tf_x = \sum_y a_{yx} f_y$$

によって定まる．この両辺を ξ に作用させると，左辺は

$$Tf_x(\xi) = \sum_z f_x(z)\psi_\xi(z) = \psi_\xi(x),$$

右辺は

$$\sum_y a_{yx} f_y(\xi) = a_{\xi x}.$$

したがって

$$a_{yx} = \psi_y(x) = \zeta^{xy} \tag{13}$$

で，$A = (\zeta^{xy})$ は次のような対称行列になる：

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots\cdots\cdots\cdots & 1 \\ 1 & \zeta & \zeta^2 & \cdots\cdots\cdots\cdots & \zeta^{p-1} \\ 1 & \zeta^2 & \zeta^4 & \cdots\cdots\cdots\cdots & \zeta^{2(p-1)} \\ & & \cdots\cdots & \cdots\cdots\cdots\cdots & \\ & & \cdots\cdots & \cdots\cdots\cdots\cdots & \\ 1 & \zeta^{p-1} & \zeta^{2(p-1)} & \cdots\cdots & \zeta^{(p-1)^2} \end{bmatrix}.$$

一方，

$$A^2 = (\zeta^{xt})(\zeta^{ty}) = \left(\sum_{t=0}^{p-1} \zeta^{t(x+y)}\right)$$

で

$$\sum_{t=0}^{p-1} \zeta^{t(x+y)} = \begin{cases} p, & x+y=0, \\ 0, & x+y \neq 0 \end{cases}$$

だから，

$$A^2 = \begin{bmatrix} p & 0 & \cdots\cdots\cdots\cdots & & 0 \\ 0 & 0 & \cdots\cdots\cdots\cdots & & p \\ 0 & 0 & \cdots\cdots\cdots & p & 0 \\ & & \cdot^{\cdot^{\cdot}} & & \\ 0 & p & & & 0 \end{bmatrix}$$

となり，

$$\det A^2 = (-1)^{p(p-1)/2} p^p,$$

よって

$$\det A = \pm i^{p(p-1)/2} p^{p/2}.$$

したがって

$$\det A = i^{p(p-1)/2} \times (\text{正の数})$$

がいえれば証明がすむ．さて，ヴァンデルモンドの定理によって，

$$\text{(14)} \qquad \det A = \prod_{0 \leqq x < y \leqq p-1} (\zeta^y - \zeta^x)$$

$$= \prod_{x<y} e^{\pi i(x+y)/p} \prod_{x<y} (e^{\pi i(y-x)/p} - e^{\pi i(x-y)/p}).$$

ここで，

$$\sum_{x<y} (x+y) = \sum_{y=1}^{p-1} \sum_{x=0}^{y-1} (x+y) = \sum_{y=1}^{p-1} \left(y^2 + \frac{y(y-1)}{2} \right) = \frac{p(p-1)^2}{2}$$

となるから，

$$\text{(14) の右辺の第 1 因子} = \prod_{0 \leqq x < y \leqq p-1} e^{\pi i(x+y)/p}$$

$$= e^{(\pi i/p)p(p-1)^2/2} = e^{\pi i(p-1)^2/2} = 1.$$

また，

$$\text{(14) の右辺の第 2 因子} = \prod_{x<y} \left(2i \sin \frac{\pi(y-x)}{p} \right)$$

$$= (2i)^{p(p-1)/2} \prod_{x<y} \sin \frac{\pi(y-x)}{p}.$$

ここで，$0 < y-x \leqq p-1$ より

$$0 < \frac{\pi(y-x)}{p} \leqq \pi\left(1-\frac{1}{p}\right) < \pi$$

だから，

$$\det A = i^{p(p-1)/2} \times (\text{正の数})$$

となる，Q.E.D.

いままでは $\mathbb{F}_p$ の加法群 $\mathbb{F}_p{}^+$ しか用いなかったが，これからやる第 2 のステップでは体 $\mathbb{F}_p$ の乗法群 $\mathbb{F}_p{}^\times$ を活用する．乗法群の指標 $\chi \in \widehat{\mathbb{F}_p{}^\times}$ は 0 では定義されていないから，

$$\chi(0) = 0$$

によって $\mathbb{F}_p$ 上の関数に拡張する．このように拡張された関数も同じ記号 χ であらわすことにする：

$$\chi \in L(\mathbb{F}_p).$$

とくに

$$\chi = \varepsilon \qquad (\mathbb{F}_p{}^\times \text{ の単位指標})$$

の場合

(15) $$\varepsilon(x) = \begin{cases} 1, & x \neq 0, \\ 0, & x = 0 \end{cases}$$

となるから，ε は 0 の特性関数を‘裏返した’ものである．いま $\mathbf{1}$ を $\mathbb{F}_p$ 上の常に値 1 をとるコンスタントとすれば，

(16) $$\varepsilon = \mathbf{1} - f_0$$

と書かれることに注意（f_x は $x \in \mathbb{F}_p$ の特性関数であった）．

さて，指標の全体 $\{\chi\}$ は $L(\mathbb{F}_p{}^\times)$ の正規直交底をなしているからもちろん独立で，したがって $\{\chi\}$ を $L(\mathbb{F}_p)$ の部分集合と見ても独立であり，$\{\chi\}$ は $L(\mathbb{F}_p)$ の超平面を張る．ところが，

$$\chi(0) = 0$$

がすべての乗法的指標 χ について成り立っているから関数 $\mathbf{1}$ はこの超平面には入らない．いい換えれば，$L(\mathbb{F}_p)$ の底として $\{\mathbf{1}, \cdots, \chi, \cdots\}$ の p 個の関数をとることができる．そこで (6) で導入した $L(\mathbb{F}_p)$ の 1 次変換 T をこの新しい

底5)で書いてみよう：

$$(17)\qquad (T\mathbf{1},\, T\varepsilon,\, \cdots) = (\mathbf{1},\, \varepsilon,\, \cdots)B.$$

命題 6　(i)　$T\mathbf{1} = p\mathbf{1} - p\varepsilon$,

(ii)　$T\varepsilon = (p-1)\mathbf{1} - p\varepsilon$.

証明　(i)　$(T\mathbf{1})(\xi) = \sum_x \mathbf{1}(x)\psi_\xi(x) = \sum_x \psi_\xi(x)$

$$= \sum_x \zeta^{\xi x} = \begin{cases} p, & \xi = 0, \\ 0, & \xi \neq 0. \end{cases}$$

したがって，

$$(T\mathbf{1})(\xi) = pf_0 = p(\mathbf{1} - \varepsilon) = p\mathbf{1} - p\varepsilon.$$

(ii)　$(T\varepsilon)(\xi) = \sum_x \varepsilon(x)\psi_\xi(x) = \sum_{x\neq 0} \psi_\xi(x) = -1 + \sum_x \psi_\xi(x)$

$$= -1 + (T\mathbf{1})(\xi) = (p-1)\mathbf{1} - p\varepsilon.$$

(i)より

$$(T\mathbf{1})(\xi) = \sum_x \psi_\xi(x) = p\mathbf{1} - p\varepsilon$$

になることを用いた，Q.E.D.

命題6から(17)の B は

$$\begin{bmatrix} p & p-1 & \\ -p & -p & \\ 0 & 0 & * \\ \vdots & \vdots & \\ 0 & 0 & \end{bmatrix}$$

の形になっている．次に $*$ の部分を定めよう．§3の定義1により $\xi \in \mathbb{F}_p$, $\chi \in \widehat{\mathbb{F}_p^\times}$, についてのガウスの和は

5)　旧い底は命題5の証明で考えた $\{f_x\}$ である．T のこの底に関する行列が A であった．

$$(18)\qquad \tau_\xi(\chi)=\sum_{x\in\mathbb{F}_p{}^\times}\chi(x)\zeta^{\xi x}=\sum_{x\in\mathbb{F}_p{}^\times}\chi(x)\psi_\xi(x)$$

であるが，$\chi(0)=0$ だから (18) の $\sum$ は $\mathbb{F}_p$ 全体でとっても変わらない．そうすれば (6) によって

$$(19)\qquad \tau_\xi(\chi)=(T\chi)(\xi),\qquad \xi\in\mathbb{F}_p,$$

とくに

$$(20)\qquad \tau(\chi)=(T\chi)(1)$$

となる．

命題 7　$\chi\neq\varepsilon$ ならば $T\chi=\tau(\chi)\bar{\chi}$.

証明　$(T\chi)(\xi)=\tau(\chi)\bar{\chi}(\xi)$

がすべての $\xi\in\mathbb{F}_p$ について成り立つことを見る．$\xi=0$ ならば右辺は $\chi(0)=0$ により 0 に等しい．また左辺は

$$(T\chi)(0)=\sum_{x\in\mathbb{F}_p}\chi(x)\psi_0(x)=\sum_{x\neq0}\chi(x)=0$$

となるからよろしい．$\xi\neq0$ のときは，(19) と§5 の命題 1 による，Q.E.D.

さて，$\chi\neq\varepsilon$ について

$$\chi=\bar{\chi}\iff\chi^2=\varepsilon$$

であり，

$$\widehat{\mathbb{F}_p{}^\times}\approx\mathbb{F}_p{}^\times$$

は巡回群だから，位数 2 の χ はただ 1 つしかない．すなわち

$$\chi=\lambda_p,\qquad \text{ルジャンドル - ガウスの指標}$$

に他ならない．$\chi\neq\varepsilon,\lambda_p$ ならば $\chi\neq\bar{\chi}$ だから，対 $\{\chi,\bar{\chi}\}$ をまとめることにして (17) を

$$(T\mathbf{1},\ T\varepsilon,\ T\lambda_p,\ T\chi,\ T\bar{\chi},\ \cdots)=(1,\varepsilon,\lambda_p,\chi,\bar{\chi},\cdots\cdots)B$$

のように書けば，B は命題 7 によって次の形となる：

$$B = \left[\begin{array}{cc|c|cc|c} p & p-1 & & & & \\ -p & -p & & & O & \\ \hline & & \tau(\lambda_p) & & & \\ \hline & & & 0 & \tau(\bar{\chi}) & \\ & & & \tau(\chi) & 0 & \\ \hline O & & & & & \ddots \end{array}\right].$$

したがって

(21)　$\det B = (-p)\tau(\lambda_p)\prod{}'(-\tau(\chi)\tau(\bar{\chi}))$

$\qquad = (-1)^{(p-1)/2}p\cdot\tau(\lambda_p)\prod{}'(\tau(\chi)\tau(\bar{\chi})).$

ただし，$\prod'$ は $\chi \neq \varepsilon, \lambda_p$ についての積で，χ としては $\{\chi, \bar{\chi}\}$ の中の1つきめた方をとるものとする[6]．(21) と§5の命題2[7]から

(22)　$\det B = (-1)^{(p-1)/2}p^{(p-1)/2}\tau(\lambda_p)\prod{}'\chi(-1)$

となる．

$p \neq 2$ だから $-1 \neq 1$，したがって $\chi_0(-1) \neq 1$ となる指標は必ずある[8]．しからば $\chi_0(-1) = -1$ でなければならない．このような χ_0 を1つきめると，写像

$$\theta \longmapsto \theta\chi_0, \qquad \theta \in \widehat{\mathbb{F}_p^\times},$$

により -1 での値の符号が入れ換わるから，$\widehat{\mathbb{F}_p^\times}$ 全体のうち -1 で値が $+1$ になるものと -1 になるものの数は同じで $(p-1)/2$ になる．

$\varepsilon(-1) = 1$ だから，$\lambda_p(-1) = 1$ ならば，$\{\chi, \bar{\chi}, \cdots\}$ の中に -1 での値が -1 になる指標が $(p-1)/2$ 個ある．$\chi(-1) = \bar{\chi}(-1)$ だから $\prod'$ のうち $(p-1)/4$ 個の χ について $\chi(-1) = -1$ になる．これに反して，$\lambda_p(-1) = -1$ ならば，$\{\chi, \bar{\chi}, \cdots\}$ の中に -1 での値が -1 になる指標が $(p-3)/2$ 個ある．したがって，$\prod'$ のうち $(p-3)/4$ 個の χ について $\chi(-1) = -1$ になる．第1補充法則（§4の定理1）によって $\lambda_p(-1) = \pm 1$ はちょうど $p \equiv \pm 1\,(4)$ に対応するから，

6）$\prod'$ にあらわれる対 $\{\chi, \bar{\chi}\}$ の数は $(p-3)/2$ であることに注意．

7）$\tau(\chi)\tau(\bar{\chi}) = \chi(-1)p.$

8）有限アーベル群 G の2元 $a \neq b$ を分離する（$\chi(a) \neq \chi(b)$ とできる）$\chi \in \widehat{G}$ が必ずとれることによる．

$$(23)\qquad \det B = \begin{cases} (-1)^{(p-1)/2}(-1)^{(p-1)/4}p^{(p-1)/2}\tau(\lambda_p), & p\equiv 1\ (4), \\ (-1)^{(p-1)/2}(-1)^{(p-3)/4}p^{(p-1)/2}\tau(\lambda_p), & p\equiv 3\ (4). \end{cases}$$

命題 5 で

$$\det B = \det T = i^{p(p-1)/2}p^{p/2}$$

がわかっているから，これと (23) とから $\tau(\lambda_p)$ を求めることができる：

$$(24)\qquad \tau(\lambda_p) = \begin{cases} (-1)^{(p-1)/2}(-1)^{(p-1)/4}i^{p(p-1)/2}\sqrt{p}, & p\equiv 1\ (4), \\ (-1)^{(p-1)/2}(-1)^{(p-3)/4}i^{p(p-1)/2}\sqrt{p}, & p\equiv 3\ (4). \end{cases}$$

これを簡単にするとガウスの定理になる，Q. E. D.

注意　本稿ではガウス以後の整数論の展開を記述するつもりはないので，ガウスの衣鉢をついだディリクレ，デデキントによる 2 次体ないし円分体における類数計算にいかにガウスの和が用いられるか，という重要な話題に触れることはできない．これについては高木貞治先生の『初等整数論講義』および『代数的整数論』(のいずれも附録) を参照されたい．そこにはガウスの和のガウス自身による符号決定も紹介されている．我々はこの連載で今までと少し違った立場から少なくとももう一度ガウスの和に遭遇する予定(？)であり，そのために §1 で少し説明した球面上の多項式の話，球面上のフーリエ解析にもどるのがよいと思う．数学の分科としては整数論から解析に引っ越すわけであるが，それは数学を今日の立場から分類した結果であって，我々はいわばそれに直交する立場からものを見ているのである．

§8．調和多項式

§1 で導入した記号を復習する[9]：

$$\mathbb{R}^n = n \text{ 次元ユークリッド空間}.$$

9）　なかには $q(x)$ のように新しい記号もある．

その点

$$x = (x_1, \cdots, x_n),$$ [10]

$$q(x) = |x|^2 = {x_1}^2 + \cdots + {x_n}^2 = \text{ベクトル } x \text{ の長さの平方},$$

$$S^{n-1} = \{\, x \in \mathbb{R}^n \,;\, q(x) = 1 \,\} = \text{原点を中心とする単位球},$$

$$P(\mathbb{R}^n) = \mathbb{R}^n \text{ 上の多項式環}.$$

$f \in P(\mathbb{R}^n)$ は $\mathbb{R}^n \longrightarrow \mathbb{R}$ なる写像で $f(x)$ が n 変数 $x = (x_1, \cdots, x_n)$ の実係数の多項式とあらわされる。

$$P_l(\mathbb{R}^n) = \{\, f \in P(\mathbb{R}^n) \,;\, f \text{ は } l \text{ 次の斉次式}\}, \qquad l \geqq 0,$$

$$P(\mathbb{R}^n) = \bigoplus_{l=0}^{\infty} P_l(\mathbb{R}^n)$$

と直和分解が成り立つ。

$$\Delta = \left(\frac{\partial}{\partial x_1}\right) + \cdots + \left(\frac{\partial}{\partial x_n}\right)^2 = \text{ラプラシアン},$$

$$H(\mathbb{R}^n) = \{\, f \in P(\mathbb{R}^n) \,;\, \Delta f = 0 \,\} = \text{調和多項式の空間},$$

$$H_l(\mathbb{R}^n) = P_l(\mathbb{R}^n) \cap H(\mathbb{R}^n\} = l \text{ 次の調和形式の空間},$$

$$H(\mathbb{R}^n) = \bigoplus_{l=0}^{\infty} H_l(\mathbb{R}^n)$$

と直和分解が成り立つ。

$P(S^{n-1})$ = **球面 S^{n-1} 上の多項式全体の空間.**

すなわち，$\varphi : S^{n-1} \longrightarrow \mathbb{R}$ が $P(S^{n-1})$ に属するとは，ある $f \in P(\mathbb{R}^n)$ があって

$$\varphi(\xi) = f(\xi), \qquad \xi \in S^{n-1}$$

となること，を意味する。

球面は平方和

$$q(x) = {x_1}^2 + \cdots + {x_n}^2$$

を 1 とおいて得られ，調和多項式は偏微分の平方和

$$\Delta = \left(\frac{\partial}{\partial x_1}\right) + \cdots\cdots + \left(\frac{\partial}{\partial x_n}\right)^2$$

---

10)　$\mathbb{R}^n$ は原点を単位元(ゼロ元)とすると $\mathbb{R}$ 加群，すなわち体 $\mathbb{R}$ 上のベクトル空間になる。

を 0 とおいて得られるから，$P(S^{n-1})$ が $H(\mathbb{R}^n)$ と関係するらしいことはほとんど明らかである．この点を明らかにすることが本節の目標である．

注意 1　$n=1$ の場合 $S^0=\{\pm 1\}$ で $H(\mathbb{R})$ は 1 次関数だけとなり，あまり面白いことは起こらない．**以下，$n \geqq 2$ と仮定する．**

注意 2　多項式とは限らず $\mathbb{R}^n \longrightarrow \mathbb{R}$ の滑らかな関数 f, g に対して Δ は線型性：

(1)　$$\Delta(\alpha f+\beta g)=\alpha \Delta f+\beta \Delta g, \qquad \alpha, \beta \in \mathbb{R}$$

をもつが，積に関して次の法則を容易に確かめることができる：

(2)　$$\Delta(fg)=f\Delta g+g\Delta f+2\langle \nabla f, \nabla g\rangle.$$

ここに ∇f は f の勾配(gradient)ベクトル

(3)　$$\nabla f=\left(\frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n}\right)$$

で，$\langle \nabla f, \nabla g\rangle$ は f, g の勾配ベクトルの内積をあらわす．

定義 1　ベクトル空間 $P_l(\mathbb{R}^n), H_l(\mathbb{R}^n)$ の次元をそれぞれ $p_l(n), h_l(n)$ と書く．

命題 1　$p_l(n)=\binom{n+l-1}{l}, \qquad l \geqq 0,\ n \geqq 2.$

証明　$P_l(\mathbb{R}^n)$ の底は単項式

$$x_1^{e_1}\cdots x_n^{e_n}, \qquad e_1+\cdots+e_n=l$$

だから，$p_l(n)$ は n 個のもの $x_1, \cdots, x_n$ から重複を許して l 個とる組合せの数に等しい，Q.E.D.

ラプラシアン $\Delta: P(\mathbb{R}^n) \longrightarrow P(\mathbb{R}^n)$ は斉次の部分に制限すると，各 $l \geqq 0$ に対して，次の写像 Δ_l をひき起こす[11)]：

(4)　$$\Delta_l: P_l(\mathbb{R}^n) \longrightarrow P_{l-2}(\mathbb{R}^n).$$

そして，明らかに

---

11)　$l=0,1$ に対してはもちろん Δ_l は 0 写像である．

$$P_{-2}(\mathbb{R}^n)=P_{-1}(\mathbb{R}^n)=\{0\}$$

と約束する．

(5)　　$\mathrm{Ker}\,\Delta_l = H_l(\mathbb{R}^n)$

であるから，完全系列：

(6)　　$0 \longrightarrow H_l(\mathbb{R}^n) \longrightarrow P_l(\mathbb{R}^n) \longrightarrow P_{l-2}(\mathbb{R}^n)$

が成り立ち，不等式

(7)　　$p_l(n) - h_l(n) \leqq p_{l-2}(n)$

を得る．実は，(6) より強く，次の完全系列が成り立つ：

(8)　　$0 \longrightarrow H_l(\mathbb{R}^n) \longrightarrow P_l(\mathbb{R}^n) \longrightarrow P_{l-2}(\mathbb{R}^n) \longrightarrow 0.$

この完全系列 (8) は次の定理 1 から出る．

ここで定理 1 の証明に必要な公式を 3 つ述べる．

(9)　　$\nabla q^{\nu} = 2\nu q^{\nu-1}\cdot x, \qquad \nu \geqq 1.$

(10)　　$\Delta q^{\nu} = 2\nu(2(\nu-1)+n)q^{\nu-1}, \qquad \nu \geqq 1.$

(11)　　$\langle \nabla g, x\rangle = (\deg g)g, \qquad g =$ 斉次式.

この 3 つを (11), (9), (10) の順に証明する．

(11) の証明．

$$\langle \nabla g, x\rangle = x_1\frac{\partial g}{\partial x_1} + \cdots\cdots + x_n\frac{\partial g}{\partial x_n}$$

だから，(11) は斉次関数についてのオイラーの公式そのものである，Q.E.D.

(9) の証明．

$$\nabla q^{\nu} = \left(\frac{\partial q^{\nu}}{\partial x_1}, \cdots, \frac{\partial q^{\nu}}{\partial x_n}\right) = \left(\nu q^{\nu-1}\frac{\partial q}{\partial x_1}, \cdots, \nu q^{\nu-1}\frac{\partial q}{\partial x_n}\right)$$

$$= \nu q^{\nu-1}\left(\frac{\partial q}{\partial x_1}, \cdots, \frac{\partial q}{\partial x_n}\right) = \nu q^{\nu-1}(2x_1, \cdots, 2x_n) = 2\nu q^{\nu-1}\cdot x,$$

Q.E.D.

(10) の証明．ν についての帰納法．$\nu = 1$ のときの主張は $\Delta q = 2n$ で，これはすぐ確かめられる．ν のときに成り立つと仮定し，公式 (2), (9) を用いると，

$$\Delta q^{\nu+1} = \Delta(q^{\nu}\cdot q) = q^{\nu}\Delta q + q\Delta q^{\nu} + 2\langle \nabla q^{\nu}, \nabla q\rangle$$
$$= 2nq^{\nu} + q2\nu(2(\nu-1)+n)q^{\nu-1} + 2\langle 2\nu q^{\nu-1}x, 2x\rangle$$

$$= 2q^{\nu}(n+\nu(2(\nu-1)+n)+4\nu)$$
$$= 2q^{\nu}(\nu+1)(n+2\nu), \qquad \text{Q.E.D.}$$

定理 1　$P_l(\mathbb{R}^n) = H_l(\mathbb{R}^n) \oplus q \cdot P_{l-2}(\mathbb{R}^n), \qquad n \geqq 2,\ l \geqq 0.$

証明　$l = 0, 1$ のときは約束により

$$P_{l-2}(\mathbb{R}^n) = \{0\}$$

で，

$$P_l(\mathbb{R}^n) = H_l(\mathbb{R}^n)$$

だから，定理は trivial に成り立つ．以下，$l \geqq 2$ と仮定する．次のことを証明する．

(12)　　$H_l(\mathbb{R}^n) \cap qP_{l-2}(\mathbb{R}^n) = 0.$

実際，$f = qg \neq 0$ が (12) の左辺にあったとする．ここに $g \in P_{l-2}(\mathbb{R}^n)$．

$$0 = \Delta f = \Delta(qg) = q\Delta g + g\Delta q + 2\langle \nabla q, \nabla g \rangle$$
$$= q\Delta g + 2ng + 2\langle 2x, \nabla g \rangle = q\Delta g + (2n+4(l-2))g.$$

$2n+4(l-2) > 0$(定数)だから，$q|g$，すなわち q は g を割る．そこで $q^{\nu} \| g$ として[12)]

$$g = q^{\nu}h$$

とおくと，$h \in P_{l-2-\nu}(\mathbb{R}^n)$ で

(13)　　$f = qg = q^{\nu+1}h \in H_l(\mathbb{R}^n)$

となる．したがって (13) の両辺の Δ をとって公式を用いれば，

$$0 = \Delta f = \Delta(q^{\nu+1}h)$$
$$= q^{\nu+1}\Delta h + h\Delta q^{\nu+1} + 2\langle \nabla q^{\nu+1}, \nabla h \rangle$$
$$= q^{\nu+1}\Delta h + h \cdot 2(\nu+1)(n+2\nu)q^{\nu} + 2\langle 2(\nu+1)q^{\nu}x, \nabla h \rangle$$
$$= q^{\nu+1}\Delta h + 2(\nu+1)(n+2\nu)hq^{\nu} + 4(\nu+1)q^{\nu}(\deg h)h$$
$$= hq^{\nu}(2(\nu+1)(n+2\nu) + 4(\nu+1)(\deg h)) + q^{\nu+1}\Delta h.$$

このことから $q|h$ となり $q^{\nu}\|g$ に矛盾する．よって (12) が成り立ち，

(14)　　$P_l(\mathbb{R}^n) \supset H_l(\mathbb{R}^n) \oplus qP_{l-2}(\mathbb{R}^n)$

---

12)　$q^{\nu} \| g$ は，$q^{\nu} | g$ だが $q^{\nu+1} \nmid g$ のこと．

となり，次元を比較して

(15)　　$p_l(n) \geqq h_l(n)+p_{l-2}(n).$

(15) と (7) から等式

(16)　　$p_l(n) = h_l(n)+p_{l-2}(n)$

が出，(14) でも等号が成り立つ．それが定理 1 である，Q.E.D.

定理 2　$h_l(n) = \dim H_l(\mathbb{R}^n) = \binom{n+l-1}{l} - \binom{n+l-3}{l-2}.$

証明　(16) と命題 1 による，Q.E.D.

定理 3 (q-展開定理)　$f \in P_l(\mathbb{R}^n)$ は次のように一意的に展開される：

$$f = \begin{cases} h_1 q^{(l-1)/2} + h_3 q^{(l-3)/2} + \cdots + h_{l-2} q + h_l, & l = \text{奇数}, \\ h_0 q^{l/2} + h_2 q^{(l-2)/2} + \cdots + h_{l-2} q + h_l, & l = \text{偶数}, \end{cases}$$

ここで $h_i \in H_i(\mathbb{R}^n)$.

証明　定理 1 を何遍も用いる，Q.E.D.

さて，はじめに定義したように球面 S^{n-1} 上の多項式全体の空間を $P(S^{n-1})$ とすると，定義により全射

(17)　　$\rho : P(\mathbb{R}^n) \longrightarrow P(S^{n-1}) \longrightarrow 0$

がある．ここに ρ は $\mathbb{R}^n$ 上の多項式を S^{n-1} に制限する写像である．ρ' で (17) の ρ を $P(\mathbb{R}^n)$ の部分空間 $H(\mathbb{R}^n)$ に制限して得られる写像とする：

(18)　　$\rho' : H(\mathbb{R}^n) \longrightarrow P(S^{n-1}).$

定理 4　(18) の写像 ρ' は全射である．すなわち任意の球面上の多項式は調和多項式の制限である．

証明　任意に $\varphi \in P(S^{n-1})$ をとる．したがって $\varphi = \rho(f)$ なる $f \in P(\mathbb{R}^n)$ がある．f の l 次の斉次部分を f_l とすると，定理 1 から

$$f_l = \begin{cases} h_1 q^{(l-1)/2} + h_3 q^{(l-3)/2} + \cdots + h_{l-2} q + h_l, & l = \text{奇数}, \\ h_0 q^{l/2} + h_2 q^{(l-2)/2} + \cdots + h_{l-2} q + h_l, & l = \text{偶数}, \end{cases}$$

$$h_i \in H_i(\mathbb{R}^n)$$

と書けるから，$q \equiv 1$ (S^{n-1} 上で) に注意すれば，

$$\rho(f_l) = \begin{cases} \rho(h_1) + \rho(h_3) + \cdots + \rho(h_l) = \rho(h_1 + h_3 + \cdots + h_l), \\ \rho(h_0) + \rho(h_2) + \cdots + \rho(h_l) = \rho(h_0 + h_2 + \cdots + h_l), \end{cases}$$

すなわち $\rho(f_l)$ は $H(\mathbb{R}^n)$ の元の制限である．φ は各 l についての $\rho(f_l)$ の和になるから，φ もある $H(\mathbb{R}^n)$ の多項式の制限になる，Q.E.D.

注意　q-展開定理(定理 3)は面白いでしょう．2 次形式 $q(x)$ と 2 次微分作用素

$$\Delta = \left(\frac{\partial}{\partial x_1}\right)^2 + \cdots + \left(\frac{\partial}{\partial x_2}\right)^2$$

を用いて任意の高次形式 ($\in P_l(\mathbb{R}^n)$) がうまく記述されることを示しています．われわれは多項式だけを扱いましたから，微分といっても代数演算で，多様体 S^{n-1} も (実) 代数多様体です．$\mathbb{R}$ をほかの体におきかえることもできるでしょう．

今回は紙数いっぱいになってしまいましたので，これでやめます．

第4回

調和多項式
球面上の積分
帯球関数

前回，整数論から解析に引っ越して調和多項式の研究を始めました．第1回の§1で $n=3$ の場合に予告してあったことを，一般の $n \geqq 2$ の場合に一歩一歩確かめることを始めたわけです．テーマは $\mathbb{R}^n$ の単位球面 S^{n-1} 上の多項式全体 $P(S^{n-1})$ と $\mathbb{R}^n$ 上の調和多項式全体 $H(\mathbb{R}^n)$ とが結局同じであるのを見ることです．

---

§9．調和多項式（つづき）

$\mathbb{R}^n$ 上の多項式環 $P(\mathbb{R}^n)$ の要素 f を球面 S^{n-1} に制限する写像を ρ とすると，$P(S^{n-1})$ の定義により ρ は全射

(1) $$\rho : P(\mathbb{R}^n) \longrightarrow P(S^{n-1}) \longrightarrow 0$$

になる．したがって完全系列：

(2) $$0 \longrightarrow \operatorname{Ker}\rho \longrightarrow P(\mathbb{R}^n) \longrightarrow P(S^{n-1}) \longrightarrow 0$$

ができる．ここで $\operatorname{Ker}\rho$ は環 $P(\mathbb{R}^n)$ のイデアルである．これはどのような多項式で生成されるであろうか？　係数体が $\mathbb{C}$（複素数体）のように代数的閉体であれば，この種の問題は有名なヒルベルトの零点定理からすぐ片付くが，我々の場合は係数体が $\mathbb{R}$（実数体）であるから，この零点定理を用いることは

できない．それよりも，S^{n-1} という $\mathbb{R}^n$ の極めて特殊な実代数多様体の性質を用いて，難しいことを何も使わない方法を工夫することにしよう．

前のように $\mathbb{R}^n$ 上の標準的2次形式を

$$q(x) = x_1{}^2 + \cdots + x_n{}^2$$

と書く．また普通のように

$$P(\mathbb{R}^n) = \mathbb{R}[x] = \mathbb{R}[x_1, \cdots, x_n]$$

と書く[1)]．

補題 $g = q-1$ は $\mathbb{R}[x]$ の既約な多項式である[2)]．

証明
$$\begin{aligned} g &= x_1{}^2 + \cdots + x_n{}^2 - 1 \\ &= (a_1x_1 + \cdots + a_nx_n + a_0)(b_1x_1 + \cdots + b_nx_n + b_0) \end{aligned}$$

と1次式の積に分解したとすると，$a_1b_1 = a_2b_2 = 1$ と $a_1b_2 + a_2b_1 = 0$ から $a_1{}^2 + a_2{}^2 = 0$ が出る．実数体 $\mathbb{R}$ を用いているから $a_1 = a_2 = 0$ となり不合理，Q.E.D.

命題1 (1), (2) の記号のもとに

$$\mathrm{Ker}\,\rho = (q-1),$$

すなわち，$\mathrm{Ker}\,\rho$ は $q-1$ の倍元全体からなる．

証明 S^{n-1} は $q(\xi) = 1$ なる $\xi \in \mathbb{R}^n$ の全体だから

$$\mathrm{Ker}\,\rho \supset (q-1)$$

は自明である．したがって $\mathrm{Ker}\,\rho \subset (q-1)$，すなわち $f(S^{n-1}) = 0$ ならば f は $g = q-1$ の倍元であることを確かめればよい．

補題により g は既約だから，f と g に $\mathbb{R}[x]$ で共通因子があることをいえば十分である．$f \neq 0$ としてよいから，f は少なくとも1つ変数 x_i を含む．変数の名前の問題だから，f は最後の変数 x_n を実際に含むとしてさしつかえない．以下 x_n を特別扱いして，

(3) $$P(\mathbb{R}^n) = \mathbb{R}[x] = \mathbb{R}[x'][x_n] \subset \mathbb{R}(x')[x_n],$$

1） 一般に，単位元をもつ可換環 A を係数とする n 変数 $x = (x_1, \cdots, x_n)$ の多項式環を $A[x_1, \cdots, x_n]$ と書く．また体 k 上の n 変数 $x = (x_1, \cdots, x_n)$ の有理関数体を $k(x_1, \cdots, x_n)$ と書く．

2） 仮定 $n \geqq 2$ に注意．

ここに

$$x' = (x_1, \cdots, x_{n-1})$$

で $\mathbb{R}(x')$ は $\mathbb{R}[x']$ の商体，とする．また簡単のため

(4)　　$K = \mathbb{R}(x') = \mathbb{R}(x_1, \cdots, x_{n-1})$

とおく．

一般に，

　'一意分解整域 R の商体を K としたとき，$R[X]$ の多項式 f, g が共通因子を持たなければ，f, g を $K[X]$ で考えても共通因子を持たない'

という多項式環のよく知られた性質[3]を用いると，我々の f, g $(g = q-1)$ が，予期に反して，$\mathbb{R}[x]$ で共通因子を持たないとすれば，$\mathbb{R}[x'][x_n]$ の多項式としてももちろん共通因子を持たず，したがって (4) により $K[x_n]$ の多項式と考えても共通因子を持たない．つまり f, g は単項イデアル環 $K[x_n]$ において互いに素である．したがって，$A_0, B_0 \in K[x_n]$ で

(5)　　$A_0 f + B_0 g = 1$

を満足するものがとれる．K は $\mathbb{R}[x']$ の商体だから $D \in \mathbb{R}[x']$，$D \neq 0$，を適当にとると A_0, B_0 の係数の分母をはらうことができ，結局

(6)　　$Af + Bg = D, \qquad A, B \in \mathbb{R}[x]$

と書ける．いま $\xi \in S^{n-1}$ を任意にとり，$\xi = (\xi', \xi_n)$ と書けば，ξ' は図6の灰色の部分(x' 平面の単位円板)にあり，ξ が S^{n-1} 上を動けば ξ' は灰色の部分全体をカヴァーする．ところで (6) から $\xi \in S^{n-1}$ ならば $g(\xi) = 0$ かつ $f(\xi) = 0$ だから

$$D(\xi) = D(\xi') = 0$$

となる．

これは，ξ' が $D = 0$ で定義される x' 平面内の実際に次元の下った(高々 $n-2$ 次元の)部分に制限されることになり，上に述べた灰色の部分を自由に動けることに矛盾する．これは，f, g が $\mathbb{R}[x]$ で共通因子を持たないと仮定したことが悪かったことを示す．したがって，予期の通り，f, g は共通因子を持ち，g が既約だから，f は $g = q-1$ の倍元になる，Q.E.D.

3） 本質的にガウスによる定理である．

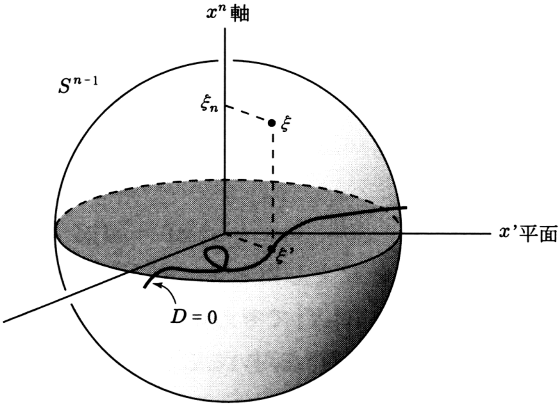


図6

前回の§8の (18) で定義したように，(1) の ρ を $H(\mathbb{R}_n)$ ($P(\mathbb{R}_m)$ の調和多項式全体からなる部分空間) に制限して得られる写像を ρ' とする．§8の定理4で ρ' は全射であることを証明した．この定理は次のように改良される．

定理 1　ρ' は

$$H(\mathbb{R}^n) \approx P(S^{n-1})$$

なるベクトル空間の同型対応を与える．

証明　ρ' が全射であることは済んでいるから，単射であることをいえばよい．

$$\mathrm{Ker}\,\rho' = H(\mathbb{R}^n) \cap \mathrm{Ker}\,\rho$$

で，命題1より $\mathrm{Ker}\,\rho = (q-1)$ だから

$$(7) \qquad H(\mathbb{R}^n) \cap (q-1) = \{0\}$$

が証明できればよい．そこで，(7) の左辺から任意に多項式をとるとそれは $f(q-1)$ の形で，条件

$$(8) \qquad \Delta(f(q-1)) = 0, \qquad f \in P(\mathbb{R}^n)$$

を満足している．これから $f=0$ を証明すればよい．

そこで $N = \deg f$ とし，

(9)　　$f=\sum_{l=0}^{N} f_l,\quad f_l\in P_l(\mathbb{R}^n)$

を f の斉次の部分への分解とする．§8 の公式 (2), (9), (10), (11) を以下自由に使用する．まず (8) を

(10)　　$\Delta(fq)=\Delta f$

と書けば，

(11)　　$\Delta(fq)=\Delta f\cdot q+f\Delta q+2\langle\nabla f,\nabla q\rangle$
$= \Delta f\cdot q+2nf+4\langle\nabla f, x\rangle=\Delta f$

となるから，(11) の両辺の l 次の部分を比較して

(12)　　$\Delta f_l\cdot q+2nf_l+4lf_l=\Delta f_{l+2},\quad 0\leqq l\leqq N$

すなわち，

(13)　　$(2n+4l)f_l+\Delta f_l\cdot q=\Delta f_{l+2},\quad 0\leqq l\leqq N.$

$l=N-1$ または N に対しては $f_{l+2}=0$ ($\deg f=N$ に注意)だから

(14)　　$(2n+4l)f_l+\Delta f_l\cdot q=0,\quad l=N-1$ または N.

いま §8 の定理 3 (q-展開定理) を f_l に用いると

(15)　　$f_l=\sum_{\nu=0}^{[l/2]} h_{l-2\nu}q^{\nu}$

となる[4]．$\Delta(h_{l-2\nu}q^{\nu})$ の計算で，§8 の $\Delta q^{\nu}, \nabla q^{\nu}$ を与える公式 (9), (10) を用いると，

(16)　　$\Delta(h_{l-2\nu}q^{\nu})=\Delta h_{l-2\nu}\cdot q^{\nu}+h_{l-2\nu}\Delta q^{\nu}+2\langle\nabla h_{l-2\nu},\nabla q^{\nu}\rangle$
$=h_{l-2\nu}\cdot 2\nu(2(\nu-1)+n)q^{\nu-1}+2\langle\nabla h_{l-2\nu}, 2\nu q^{\nu-1}\cdot x\rangle$
$=h_{l-2\nu}q^{\nu-1}\cdot 2\nu(2(\nu-1)+n)+4\nu q^{\nu-1}(l-2\nu)h_{l-2\nu}$
$=A_{\nu}h_{l-2\nu}q^{\nu-1},$

ここに

(17)　　$A_{\nu}=2\nu(2(\nu-1)+n)+4\nu(l-2\nu)>0.$[5]

(15), (17) を (14) に代入して，

4）［a］は a を越えない最大の整数をあらわす(ガウスの記号)．(15) は §8，定理 3 の 2 つの式を l の偶，奇に分けずに同時に書いたものである．

5） (15), (16), (17) は任意の l，$0\leqq l\leqq N$，に対して成り立つ．

(18) $\displaystyle\sum_{\nu=0}^{[l/2]}((2n+4l)+A_\nu)h_{l-2\nu}q^\nu=0$

となる．q-展開の一意性から

(19) $((2n+4l)+A_\nu)h_{l-2\nu}=0, \qquad 0\leqq\nu\leqq\left[\dfrac{l}{2}\right],$

あるいは

(20) $h_{l-2\nu}=0, \qquad 0\leqq\nu\leqq\left[\dfrac{l}{2}\right]$

となり，結局

(21) $f_l=0, \qquad l=N-1$ または N

が出た．これができると，(21) を (13) に入れて

(22) $(2n+4l)f_l+\Delta f_l\cdot q=0, \qquad l=N-3$ または $N-2$

が出る．すると (14) から (21) を出したのと同じ手続きで (22) から

(23) $f_l=0, \qquad l=N-3$ または $N-2$

が出る．以下，同様にくり返すと，結局

(24) $f_l=0, \qquad 0\leqq l\leqq N,$

すなわち $f=0$，Q.E.D.

定理 1 の同型対応

$$\rho':H(\mathbb{R}^n)\approx P(S^{n-1})$$

を $H(\mathbb{R}^n)$ の l 次の部分 $H_l(\mathbb{R}^n)$ に制限すると，同型対応

(25) $\rho_l':H_l(\mathbb{R}^n)\approx H_l(S^{n-1})$

を得る．ここで ρ_l' の像を $H_l(S^{n-1})$ と書いたのである．

$$H(\mathbb{R}^n)=\bigoplus_{l=0}^{\infty}H_l(\mathbb{R}^n)$$

の直和分解が次の直和を導く：

(26) $\displaystyle P(S^{n-1})=\bigoplus_{l=0}^{\infty}H_l(S^{n-1}).$

注意 これで §1 で予告した結果 (9) およびその任意の $n\geqq 2$ への拡張が片付いたわけで，次の課題は $H_l(S^{n-1})$ の底をルジャンドル多項式を用いて書き

あらわすこと(§1の(10)の $n \geqq 2$ への拡張)である．我々は $n \geqq 2$ の場合の拡張された意味のルジャンドル多項式をほとんど代数的な手続きのみを用いて導入する．したがって我々の意味で定義されたルジャンドル多項式が $n=3$ の場合にルジャンドルの意味でのルジャンドル多項式と同じかどうかは検討を要するところである．いずれにせよ S^{n-1} 上の積分を用いて (26) の直和分解を研究せねばならない．

§10．球面上の積分

n 次元ユークリッド空間 $\mathbb{R}^n$ の中で

(1) $$B^n = \{ x \in \mathbb{R}^n ; q(x) \leqq 1 \}$$

が原点を中心とした単位球で，

(2) $$S^{n-1} = \{ \xi \in \mathbb{R}^n ; q(\xi) = 1 \}$$

が原点を中心とした単位球面である．S^{n-1} は B^n の境界で $S^{n-1} = \partial B^n$ とも書かれる．dx で B^n における体積要素，$d\xi$ で S^{n-1} における面積要素をあらわす．B^n の点 x は

(3) $$x = r\xi, \qquad 0 \leqq r \leqq 1, \xi \in S^{n-1}$$

と書かれ，微分については

(4) $$dx = r^{n-1} dr d\xi$$

という関係にある．いま U を B^n を含む $\mathbb{R}^n$ の開集合とし，

(5) $$F : U \longrightarrow \mathbb{R}^n$$

を滑らかな写像，すなわち U で定義されたベクトル場とし，ν を S^{n-1} 上の外向きの単位法線ベクトル場とすると，次のガウス‐グリーンの公式が成り立つ：

(6) $$\int_{B^n} \operatorname{div} F dx = \int_{S^{n-1}} \langle F, \nu \rangle d\xi,$$

ここで

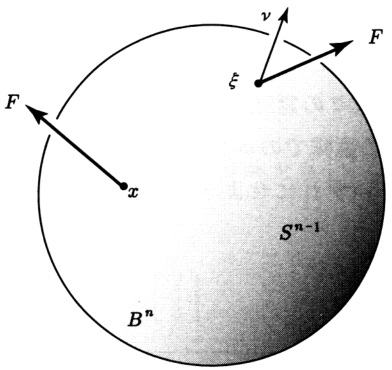


図 7

(7) $$\operatorname{div} F = \frac{\partial F_1}{\partial x_1} + \cdots + \frac{\partial F_n}{\partial x_n} \qquad \text{(発散)}$$

である．ただし，$F = (F_1, \cdots, F_n)$．

命題 1 U を B^n を含む $\mathbb{R}^n$ の開集合，f, g を U で定義された滑らかな関数とすると

$$\int_{B^n} (g\Delta f - f\Delta g)dx = \int_{S^{n-1}} \langle g\nabla f - f\nabla g, \nu\rangle d\xi$$

が成り立つ．

証明 $$F = g\nabla f = \left(g\frac{\partial f}{\partial x_1}, \cdots, g\frac{\partial f}{\partial x_n}\right)$$

は U 上のベクトル場である．そして

(8) $$\operatorname{div} F = g\Delta f + \langle \nabla f, \nabla g\rangle$$

となるから，(8) を (6) に代入して

(9) $$\int_{B^n} g\Delta f dx + \int_{B^n} \langle \nabla f, \nabla g\rangle dx = \int_{S^{n-1}} \langle g\nabla f, \nu\rangle d\xi.$$

(9) で f と g をとりかえると，

(10) $$\int_{B^n} f\Delta g dx + \int_{S^{n-1}} \langle \nabla g, \nabla f\rangle dx = \int_{S^{n-1}} \langle f\nabla g, \nu\rangle d\xi.$$

$\langle\nabla f, \nabla g\rangle = \langle\nabla g, \nabla f\rangle$ だから，(9) から (10) を引けばよい，Q.E.D.

さて，$P(S^{n-1})$ に次のように内積を定義する．

$$(11) \qquad \langle\varphi, \psi\rangle = \int_{S^{n-1}} \varphi(\xi)\psi(\xi)d\xi, \qquad \varphi, \psi \in P(S^{n-1}).$$

命題 2　$\varphi \in H_l(S^{n-1})$, $\psi \in H_k(S^{n-1})$ で $l \neq k$ とすれば

$$\langle\varphi, \psi\rangle = 0.$$

すなわち，§ 9 の (26) の直和分解

$$P(S^{n-1}) = \bigoplus_{l=0}^{\infty} H_l(S^{n-1})$$

は直交分解である．

証明　§ 9 の (25) の同型対応で φ に対応する l 次の調和形式を $f \in H_l(\mathbb{R}^n)$, ψ に対応する k 次の調和形式を $g \in H_k(\mathbb{R}^n)$ とする．すなわち，φ は f の S^{n-1} への制限で，ψ は g の S^{n-1} への制限である．$\Delta f = \Delta g = 0$ だから，命題 1 より

$$(12) \qquad \int_{S^{n-1}} \langle g\nabla f - f\nabla g, \nu\rangle d\xi = 0.$$

さて

$$\langle\nabla f, \nu\rangle = \langle\nabla f, \xi\rangle^{6)} = lf, \qquad \langle\nabla g, \nu\rangle = kg$$

だから，(12) は

$$(13) \qquad 0 = \int_{S^{n-1}} (glf - fkg)d\xi = (l-k)\int_{S^{n-1}} \varphi\psi d\xi = (l-k)\langle\varphi, \psi\rangle$$

となる．$l \neq k$ だから $\langle\varphi, \psi\rangle = 0$，Q.E.D.

注意　このようにして，球面上の多項式全体の空間の研究は内積 $\langle\ ,\ \rangle$ を持った**球面調和関数**の空間 $H_l(S^{n-1})$ の研究に帰せられたのである．

6）S^{n-1} 上の点 ξ における外向き法線ベクトル ν は ξ にほかならない．

§ 11. 帯球関数

$l \geqq 0$ に対して l 次の調和形式全体 $H_l(\mathbb{R}^n)$ は，§ 8 の定理 2 により次元が

(1) $$h_l(n) = \binom{n+l-1}{l} - \binom{n+l-3}{l-2}$$

の $\mathbb{R}$ 上のベクトル空間であった．以下，簡単のために

(2) $$N = h_l(n)$$

とおく．同型対応

$$H_l(\mathbb{R}^n) \approx H_l(S^{n-1}) \qquad (§\,9,\ (25))$$

によって $H_l(S^{n-1})$ も内積 $\langle\ ,\ \rangle$ をもつ N 次元のユークリッド空間になる[7]．

$\mathbb{R}^n$ の直交群 $O(\mathbb{R}^n)$ から σ をとり

(3) $$(\sigma^*\varphi)(\xi) = \varphi(\sigma^{-1}\xi), \qquad \varphi \in H_l(S^{n-1}), \quad \xi \in S^{n-1}$$

とおく．直交群は S^{n-1} に作用するから (3) の右辺は意味をもつ．したがって，S^{n-1} 上の関数 $\sigma^*\varphi$ が (3) によって定義される．一方，φ が $f \in H_l(\mathbb{R}^n)$ の S^{n-1} への制限であるとすれば，(3) と同様に，$\sigma \in O(\mathbb{R}^n)$ に対して

(4) $$(\sigma^*f)(x) = f(\sigma^{-1}x), \qquad x \in \mathbb{R}^n$$

によって $\sigma^*f \in P_l(\mathbb{R}^n)$ が定まるが，

(5) $$\Delta(\sigma^*f) = \sigma^*(\Delta f), \qquad \sigma \in O(\mathbb{R}^n)$$

が容易に確かめられるので，$\Delta f = 0$ から $\Delta(\sigma^*f) = 0$，すなわち $\sigma^*f \in H_l(\mathbb{R}^n)$ が出る．(3) にもどれば，これは $\sigma^*\varphi \in H_l(S^{n-1})$ を意味する．

命題 1 $\sigma \longmapsto \sigma^*$ は

$$O(\mathbb{R}^n) \longrightarrow O(H_l(S^{n-1}))$$

なる準同型写像を与える．

7）同型対応 $H_l(\mathbb{R}^n) \approx H_l(S^{n-1})$ によって対応する関数をしばしば同一視する．たとえば，$\varphi(\xi) \in H_l(S^{n-1})$ に対して

$$\varphi(x), \qquad x \in \mathbb{R}^n$$

と書いたときは，φ を無言のうちに自然に $H_l(\mathbb{R}^n)$ の斉次多項式と見ていることになる．

証明　上の考察により $\sigma^* \in GL(H_l(S^{n-1}))$ はよろしい．また $\sigma, \tau \in O(\mathbb{R}^n)$ に対して

$$(\sigma\tau)^* = \sigma^*\tau^*$$

になることも定義 (3) から明らかである．したがって

$$\langle \sigma^*\varphi, \sigma^*\psi \rangle = \langle \varphi, \psi \rangle \tag{6}$$

を証明すればよい．実際，

$$\langle \sigma^*\varphi, \sigma^*\psi \rangle = \int_{S^{n-1}} (\sigma^*\varphi)(\xi)(\sigma^*\psi)(\xi)d\xi = \int_{S^{n-1}} \varphi(\sigma^{-1}\xi)\psi(\sigma^{-1}\xi)d\xi$$

$$= \int_{S^{n-1}} \varphi(\xi)\psi(\xi)d\xi = \langle \varphi, \psi \rangle$$

が，$d\xi$ が $O(\mathbb{R}^n)$ 不変という事実から出るからよろしい，Q.E.D.

さて，ユークリッド空間 $(H_l(S^{n-1}), \langle\ ,\ \rangle)$ の正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ を 1 つ選んで

$$F(\xi, \eta) = \sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\eta), \qquad \xi, \eta \in S^{n-1} \tag{7}$$

なる $S^{n-1} \times S^{n-1}$ 上の関数を考える．

命題 2　$F(\sigma\xi, \sigma\eta) = F(\xi, \eta), \qquad \sigma \in O(\mathbb{R}^n), \quad \xi, \eta \in S^{n-1}$

証明　σ の代りに σ^{-1} を用いて，

$$F(\sigma^{-1}\xi, \sigma^{-1}\eta) = \sum \varphi_i(\sigma^{-1}\xi)\varphi_i(\sigma^{-1}\eta) = \sum (\sigma^*\varphi_i)(\xi)(\sigma^*\varphi_i)(\eta).$$

命題 1 から σ^* もユークリッド空間 $H_l(S^{n-1})$ の直交変換だから，N 次の正方行列 T を

$$(\sigma^*\varphi_1, \cdots, \sigma^*\varphi_N) = (\varphi_1, \cdots, \varphi_N)T$$

によって定めれば T は直交行列になる：

$$T^tT = 1, \qquad 1 \text{ は } N \text{ 次の単位行列.} \tag{8}$$

したがって，(8) を用いて，

$$F(\sigma^{-1}\xi, \sigma^{-1}\eta) = \sum_{i=1}^{N} (\sigma^*\varphi_i)(\xi)(\sigma^*\varphi_i)(\eta)$$

$$= ((\sigma^*\varphi_1)(\xi), \cdots, (\sigma^*\varphi_N)(\xi))\begin{pmatrix}(\sigma^*\varphi_1)(\eta)\\ \vdots \\ (\sigma^*\varphi_N)(\eta)\end{pmatrix}$$

$$= (\varphi_1(\xi), \cdots, \varphi_N(\xi))\, T\, {}^tT\begin{pmatrix}\varphi_1(\eta)\\ \vdots \\ \varphi_N(\eta)\end{pmatrix}$$

$$= (\varphi_1(\xi), \cdots, \varphi_N(\xi))\begin{pmatrix}\varphi_1(\eta)\\ \vdots \\ \varphi_N(\eta)\end{pmatrix}$$

$$= \sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\eta) = F(\xi, \eta), \qquad \text{Q.E.D.}$$

命題 3　(7) で定義された $F : S^{n-1}\times S^{n-1} \longrightarrow \mathbb{R}$ は，定義に用いた正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ のとり方によらずユークリッド空間 $(H_l(S^{n-1}), \langle\ ,\ \rangle)$ だけによって定まる．

証明　$\{\psi_1, \cdots, \psi_N\}$ をもう 1 つの正規直交底とする．したがって N 次の直交行列 T があって

$$(\psi_1, \cdots, \psi_N) = (\varphi_1, \cdots, \varphi_N)\, T$$

となる．さて，

$$\sum_{i=1}^{N} \psi_i(\xi)\psi_i(\eta) = (\psi_1(\xi), \cdots, \psi_N(\xi))\begin{pmatrix}\psi_1(\eta)\\ \vdots \\ \psi_N(\eta)\end{pmatrix}$$

$$= (\varphi_1(\xi), \cdots, \varphi_N(\xi))\, T\, {}^tT\begin{pmatrix}\varphi_1(\eta)\\ \vdots \\ \varphi_N(\eta)\end{pmatrix}$$

$$= (\varphi_1(\xi), \cdots, \varphi_N(\xi))\begin{pmatrix}\varphi_1(\eta)\\ \vdots \\ \varphi_N(\eta)\end{pmatrix} = \sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\eta)$$

となるから，Q.E.D.

以下，$\varepsilon_1, \cdots, \varepsilon_{n-1}, \varepsilon_n$ で $\mathbb{R}^n$ の標準的正規直交底，すなわち

(9)　$$\varepsilon_i = (0, \cdots, \overset{i}{\overbrace{1}}, \cdots, 0), \qquad 1 \leqq i \leqq n$$

とする．

$$x = (x_1, \cdots, x_n) = x_1\varepsilon_1 + \cdots + x_{n-1}\varepsilon_{n-1} + x_n\varepsilon_n$$

であり，§9 でやったように，x に対して，

(10)　$$x' = (x_1, \cdots, x_{n-1}) = x_1\varepsilon_1 + \cdots + x_{n-1}\varepsilon_{n-1}$$

と書く．いい換えれば，$\varepsilon_1, \cdots, \varepsilon_{n-1}$ は x_n 軸に直交する x' 平面を張る．

(11)　$$x' \longmapsto (x', 0)$$

の対応で $\mathbb{R}^{n-1} \subset \mathbb{R}^n$ と考える．$\sigma \in O(\mathbb{R}^n)$ が ε_n を動かさなければ $\sigma' \in O(\mathbb{R}^{n-1})$ が定まって

(12)　$$\sigma x = \sigma(x', x_n) = (\sigma' x', x_n)$$

となる．逆に，(11), (12) によって $O(\mathbb{R}^{n-1})$ は自然に $O(\mathbb{R}^n)$ の部分群になる．

定義 1　$\varphi \in H_l(S^{n-1})$ で，$\sigma\varepsilon_n = \varepsilon_n$ となる $\sigma \in O(\mathbb{R}^n)$ に対してはつねに

$$\sigma^*\varphi = \varphi$$

となるものの全体を $Z_l(S^{n-1})$ と書く．$Z_l(S^{n-1})$ の関数を (l, n) に関する**帯球関数**という．

注意 1　(12) によって $O(\mathbb{R}^{n-1}) \subset O(\mathbb{R}^n)$ と見れば

(13)　$$Z_l(S^{n-1}) = \{\, \varphi \in H_l(S^{n-1});\, \sigma^*\varphi = \varphi,\ \sigma \in O(\mathbb{R}^{n-1})\}$$

とあらわされる．$\varphi \equiv 0$ はもちろん $Z_l(S^{n-1})$ の元であるから $Z_l(S^{n-1})$ は空集合ではなく，$H_l(S^{n-1})$ のある部分空間(帯球関数の空間)である．次の定理がルジャンドル多項式の理論の基礎である．

定理 1　$Z_l(S^{n-1})$ は 1 次元の実ベクトル空間である．

証明　存在と一意性の 2 つの部分から成る．

まず，0 でない帯球関数が少なくとも 1 つ存在することを見よう．定義 (7) の $F(\xi, \eta)$ で $\eta = \varepsilon_n$ とおくと

(14)　$$f(\xi) = F(\xi, \varepsilon_n) = \sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\varepsilon_n)$$

で与えられる f は $H_l(S^{n-1})$ に属する[8]．$\sigma \in O(\mathbb{R}^{n-1})$ ならば，命題 2 を用いて，

8）　$f = \sum \varphi_i(\varepsilon_n)\varphi_i$ で $\varphi_i \in H_l(S^{n-1})$ だから．

$$f(\sigma\xi)=F(\sigma\xi,\varepsilon_n)=F(\sigma\xi,\sigma\varepsilon_n)=F(\xi,\varepsilon_n)=f(\xi)$$

となるから $f\in Z_l(S^{n-1})$．次に，命題 2 から，

$$f(\varepsilon_n)=F(\varepsilon_n,\varepsilon_n)=F(\xi,\xi),\qquad \xi\in S^{n-1}.$$

したがって，a_{n-1} を S^{n-1} の表面積とすると，

$$f(\varepsilon_n)a_{n-1}=\int_{S^{n-1}}f(\varepsilon_n)d\xi=\int_{S^{n-1}}F(\xi,\xi)d\xi$$

$$=\int_{S^{n-1}}\sum_{i=1}^{N}\varphi_i(\xi)\varphi_i(\xi)d\xi=\sum_{i=1}^{N}\langle\varphi_i,\varphi_i\rangle=N,$$

したがって $f(\varepsilon_n)\neq 0$，すなわち $f\neq 0\in Z_l(S^{n-1})$ がみつかった．

次に一意性の証明であるが，2 つの補題をやっておこう．

補題 1 $f\in P_l(\mathbb{R}^n)$ が

$$\sigma^*f=f,\qquad \sigma\in O(\mathbb{R}^n)$$

を満足していれば

$$f=cq^{l/2},\qquad l \text{ は偶数},\ q=x_1{}^2+\cdots+x_n{}^2.$$

補題 1 の証明 $f\neq 0$ としてよい．$O(\mathbb{R}^n)$ は S^{n-1} に推移的に作用するから，f は S^{n-1} 上では定数である．$x=r\xi$ と書けば

$$f(x)=r^lf(\xi)=cq^{l/2},\qquad f(\xi)=c$$

となる．q は，$n\geqq 2$ のとき $\mathbb{R}[x]$ で既約だから，$f(x)$ が多項式であるためには l は偶数でなければならない，補題 1 の Q.E.D.[9)]

補題 2 $g(x)\in P_l(\mathbb{R}^n)$ を

$$x=(x',x_n),\qquad x'=(x_1,\cdots,x_{n-1})$$

によって

$$g(x)=\sum_{j=0}^{l}g_{l-j}(x')x_n{}^j,\qquad g_{l-j}\in P_{l-j}(\mathbb{R}^{n-1})$$

と書き，ラプラシアンについても

$$\Delta=\Delta'+\left(\frac{\partial}{\partial x_n}\right)^2,\qquad \Delta'=\left(\frac{\partial}{\partial x_1}\right)^2+\cdots+\left(\frac{\partial}{\partial x_{n-1}}\right)^2$$

9） §9 の補題の証明と同様にすぐできる．もしも l が奇数とすると，$f=cq^{l/2}$ の両辺を平方して $f^2=c^2q^l$．ここで q は既約だから分解の一意性から f は q の巾で，f^2 が q の偶数巾となり不合理．

と約束すると，

$$\Delta g=0 \iff (\#)\begin{cases}\Delta' g_l + 1\cdot 2 g_{l-2}=0,\\ \Delta' g_{l-1}+2\cdot 3 g_{l-3}=0,\\ \Delta' g_{l-2}+3\cdot 4 g_{l-4}=0,\\ \quad\cdots\cdots\cdots\cdots\\ \Delta' g_2+(l-1)l g_0=0.\end{cases}$$

補題 2 の証明

$$\Delta(g_{l-j}(x')x_n^j)=\Delta'(g_{l-j}(x')x_n^j)+\left(\frac{\partial}{\partial x_n}\right)^2(g_{l-j}(x')x_n^j)$$
$$=x_n^j\Delta' g_{l-j}+j(j-1)x_n^{j-2}g_{l-j}$$

より

$$\Delta g=\sum_{j=0}^{l}x_n^j\Delta' g_{l-j}+\sum_{j=0}^{l-2}(j+1)(j+2)x_n^j g_{l-j-2}$$
$$=\sum_{j=0}^{l-2}x_n^j((j+1)(j+2)g_{l-j-2}+\Delta' g_{l-j})\ ^{10)}$$

となるから，補題 2 の Q.E.D.

さて，定理 1 の証明にもどって，$f\in Z_l(S^{n-1})$ を任意にとり補題 2 にならって

(15)　$$f(x)=\sum_{j=0}^{l}f_{l-j}(x')x_n^j,\qquad f_{l-j}\in P_{l-j}(\mathbb{R}^{n-1})$$

と書く．

$$\sigma^* f=f,\qquad \sigma\in O(\mathbb{R}^{n-1})$$

だから

$$\sigma x=(\sigma x', x_n)$$

に注意すれば，(15) から

(16)　$$f_{l-j}(\sigma x')=f_{l-j}(x'),\qquad \sigma\in O(\mathbb{R}^{n-1})$$

となり，補題 1 により，(16) から

(17)　$$f_{l-j}(x')=c_{l-j}q(x')^{(l-j)/2},$$

10)　$\Delta' g_0=\Delta' g_1=0$ に注意．

ただし $c_{l-j} \neq 0$ のときは $l-j$ は偶数，となる．いい換えれば (15) は

$$(18) \qquad f(x) = \sum_{l-j\equiv 0(2)} x_n{}^j c_{l-j} q(x')^{(l-j)/2}$$

と書くことができる．一方，$\Delta f = 0$ であるから，補題 2 により ($g_{l-j}(x') = c_{l-j}q(x')^{(l-j)/2}$ として)

$$(19) \qquad c_{l-j}\Delta' q(x')^{(l-j)/2} + (j+1)(j+2)c_{l-j-2}q(x')^{(l-j-2)/2} = 0, \quad 0 \leqq j \leqq l-2$$

となり，§8 の公式 (10)[11]を $q(x')$ に用いれば，(19) は

$$(20) \qquad (l-j)(l-j-2+n-1)c_{l-j} + (j+1)(j+2)c_{l-j-2} = 0, \quad 0 \leqq j \leqq l-2$$

となる．したがって $j = l-2$，すなわち c_0 から出発して $l-j \equiv 0\,(2)$ となる c_{l-j} は (20) により順々に定まり[12]，(18) の $f(x)$ は c_0 の選び方で定まってしまう[13]．これは

$$\dim Z_l(S^{n-1}) \leqq 1$$

を意味する．一方，$\dim Z_l(S^{n-1}) \geqq 1$ は前半で済んでいるから，Q.E.D.

今回も与えられた紙数いっぱいになってしまいました．もうひと息でルジャンドル多項式 $P_{l,n}(t)$ の定義ができます．

---

11) $\Delta q^\nu = 2\nu(2(\nu-1)+n)q^{\nu-1}$.

12) (20) の各係数

$$(l-j)(l-j-2+n-1), \qquad (j+1)(j+2)$$

は >0 になることに注意．

13) つまり c_{l-j} は c_0 の定数倍になる．

第5回

ルジャンドル多項式の定義
直交多項式系
$n=2$ の場合

前回，帯球関数の空間 $Z_l(S^{n-1})$ が1次元であることを証明しました．今回はこの応用として，ルジャンドル多項式 $P_{l,n}(t)$ を定義し，n を固定したとき $\{P_{l,n}(t)\}$ が直交多項式系をなすことを証明し，古典的な場合との関連を明らかにしましょう．

§12．ルジャンドル多項式の定義

$l \geqq 0$ に対して，l 次の調和形式全体の空間 $H_l(\mathbb{R}^n)$ は，その要素 f を S^{n-1} に制限することにより，球面調和関数全体の空間 $H_l(S^{n-1})$ を導いた．そしてこの制限する写像は同型対応

(1) $\qquad H_l(\mathbb{R}^n) \approx H_l(S^{n-1})$

を与えた．今まで通り，われわれはこの2つの空間(それらは S^{n-1} 上の積分で与えられる内積 $\langle\ ,\ \rangle$ によりユークリッド空間でもあったが)を自由に同一視する．$\mathbb{R}^n$ の点を x，S^{n-1} の点を ξ と一般に区別することも前の通り．また $x=(x_1, \cdots, x_n) \in \mathbb{R}^n$ を

$$x=(x', x_n), \qquad x'=(x_1, \cdots, x_{n-1}) \in \mathbb{R}^{n-1}$$

とあらわし，$O(\mathbb{R}^{n-1})$ を自然に $O(\mathbb{R}^n)$ の部分群と考える．すなわち，$\sigma' \in$

$O(\mathbb{R}^{n-1})$ に対して

$$\sigma x = (\sigma' x', x_n)$$

によって得た $\sigma \in O(\mathbb{R}^n)$ を σ' と同一視する．もう１つ，$\sigma \in (\mathbb{R}^n)$ に対して

$$\sigma^* \varphi(\xi) = \varphi(\sigma^{-1}\xi), \qquad \xi \in S^{n-1},\ \varphi \in H_l(S^{n-1})$$

により σ^* を定める．以上の記号のもとに

(2) $\qquad Z_l(S^{n-1}) = \{\, \varphi \in H_l(S^{n-1})\,;\, \sigma^*\varphi = \varphi,\ \varphi \in O(\mathbb{R}^{n-1})\,\}$

によって (l, n) に関する帯球関数全体の空間を定義し，

(3) $\qquad \dim Z_l(S^{n-1}) = 1 \qquad$ (§11 の定理 1)

を証明した．

さて，(3) により $Z_l(S^{n-1})$ には 0 でない関数 f があるわけで，さらに §11 の定理 1 の証明(の前半)によれば

(4) $\qquad f(\varepsilon_n) \neq 0, \qquad \varepsilon_n = (0, \cdots, 0, 1)$

なる f がある．したがって

(5) $\qquad f(\varepsilon_n) = c_0 \neq 0$

とおく[1)]．しからば

$$(c_0^{-1}f)(\varepsilon_n) = 1, \qquad c_0^{-1}f \in Z_l(S^{n-1})$$

で，この‘初期条件’によって帯球関数は一意的に定まる．

定義 1 上の議論によって一意的に定まる帯球関数を $\lambda_{l,n}$ と書く．したがって，

$$\lambda_{l,n} \in Z_l(S^{n-1}), \qquad \lambda_{l,n}(\varepsilon_n) = 1. \qquad \text{(定義終)}$$

§11 の (7) で $(H_l(S^{n-1}), \langle\ ,\ \rangle)$ の任意の正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ に対して

(6) $\qquad F(\xi, \eta) = \sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\eta), \qquad \xi, \eta \in S^{n-1}$

なる $S^{n-1} \times S^{n-1}$ 上の関数を定義した．そして，§11 の定理 1 の証明の前半によれば

1) この c_0 は §11 の式 (18) にあらわれる c_0 になる．このことは §11，定理 1 が証明された今となっては忘れてもよいのであるが，一方，§11 の式 (20) のように，すべての c_{l-j} が c_0 からきまるという事実は有力である．

$$(7)\qquad f(\xi)=F(\xi,\,\varepsilon_n)=\sum_{i=1}^{N}\varphi_i(\xi)\varphi_i(\varepsilon_n)$$

とおいて定まる f が $Z_l(S^{n-1})$ の要素で

$$(8)\qquad f(\varepsilon_n)=\frac{N}{a_{n-1}},\qquad a_{n-1}=\int_{S^{n-1}}d\xi$$

であった．したがって次の命題を得る．

命題 1　$\lambda_{l,n}(\xi)=\dfrac{a_{n-1}}{N}F(\xi,\,\varepsilon_n).$

証明　$\lambda_{l,n}(\xi), F(\xi,\,\varepsilon_n)$ ともに $Z_l(S^{n-1})$ の関数で

$$\lambda_{l,n}(\varepsilon_n)=1,\qquad \frac{a_{n-1}}{N}F(\varepsilon_n,\,\varepsilon_n)=1$$

となるから，$\dim Z_l(S^{n-1})=1$ による，Q.E.D.

一方，§11 の定理 1 の証明の後半によれば，そこの式 (18) により

$$(9)\qquad \lambda_{l,n}(x)=\sum_{l-j\equiv 0(2)}c_{l-j}x_n{}^j q(x')^{(l-j)/2},\qquad 0\leqq j\leqq l$$

と書ける．ここで $\lambda_{l,n}(\varepsilon_n)=1$ ということは $c_0=1$ を意味する $(x=\varepsilon_n=(0,\cdots,0,1),\ x'=(0,\cdots,0)\in\mathbb{R}^{n-1},\ x_n=1)$．したがって，§11 の式 (20) を用いれば，次の命題を得る．

命題 2　$\lambda_{l,n}(x)=\displaystyle\sum_{l-j\equiv 0(2)}c_{l-j}x_n{}^j q(x')^{(l-j)/2},\qquad 0\leqq j\leqq l,\ c_0=1$

であり，$0\leqq j\leqq l-2$ に対して関係

$$(10)\qquad (l-j)(l-j-2+n-1)c_{l-j}+(j+1)(j+2)c_{l-j-2}=0$$

が成り立つ．

注意 1　$c_0=1$ だから公式 (10) から各 c_{l-j} が順々に定まり，c_{l-j} が c_0 の定数倍になる．この定数を決定することは容易だが，ここでは実行しない．(注意終)

さて，$\xi \in S^{n-1}$ に対して $\sigma \in O(\mathbb{R}^{n-1})$ を適当にとると，ξ を x_n 軸のまわりに廻転させて $\sigma\xi$ が $\varepsilon_{n-1}, \varepsilon_n$ の張る平面，すなわち (x_{n-1}, x_n) 平面に含まれるようにすることができる．$\lambda_{l,n}(\xi)$ は帯球関数だから

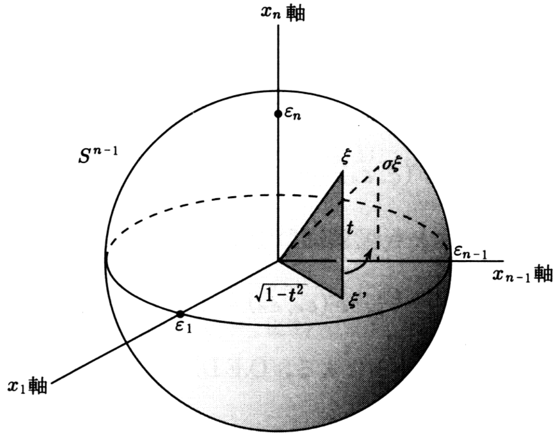


図 8

$$\lambda_{l,n}(\xi) = \lambda_{l,n}(\sigma\xi)$$

で，

$$\text{(11)} \qquad \sigma\xi = \sqrt{1-t^2}\,\varepsilon_{n-1} + t\varepsilon_n, \qquad -1 \leqq t \leqq 1$$

だから，

$$x = \sigma\xi = (0, \cdots, 0, \sqrt{1-t^2}, t)$$

として命題 2 を用いれば

$$\text{(12)} \qquad \lambda_{l,n}(\xi) = \sum_{l-j\equiv 0(2)} c_{l-j} t^j (1-t^2)^{(l-j)/2}, \qquad 0 \leqq j \leqq l$$

と書くことができる．ここで t は $-1 \leqq t \leqq 1$ なる実数であるが，右辺は t についての多項式であるから，次の定義を得る．

定義 2　$l \geqq 0,\ n \geqq 2$ に対して 1 変数 t の多項式

$$P_{l,n}(t) = \sum_{l-j\equiv 0(2)} c_{l-j} t^j (1-t^2)^{(l-j)/2}, \qquad 0 \leqq j \leqq l$$

のことを (l, n) の定める**ルジャンドル多項式**という．ここに，$c_0=1$ であり，$0 \leqq j \leqq l-2$ に対して関係式

$$(l-j)(l-j-2+n-1)c_{l-j}+(j+1)(j+2)c_{l-j-2}=0$$

が成り立っているものとする．

注意2　我々は実代数多様体 S^{n-1} 上の解析学をユックリやりながら上の定義2に到着した．ところで，定義だけなら，このような準備は何一ついらない．$P_{l,n}(t)$ は定義に述べた条件で完全に定まる極めて明快な1変数 t の多項式である．もし数学が名前(たとえばルジャンドル多項式)と論理のみからなるならば，中学生にもわかる定義2が $P_{l,n}(t)$ すべてを所有しているわけで，連載などしないでも原稿用紙1枚ですむことである．しかし，何の前触れもなく，突如として定義2を与えられたら，よほど信心深いか，被虐愛好家でもない限り，嫌悪を催すだけであろう．(注意終)

次に，定義のいい換えを命題として述べる．

命題3　$P_{l,n}(t)=\lambda_{l,n}(\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n)=\dfrac{a_{n-1}}{N}F(\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n, \varepsilon_n).$

証明　命題1，命題2から明らか，Q.E.D.

注意3　命題3にあらわれる F，すなわち§11の (7) で定義した関数 F : $S^{n-1}\times S^{n-1} \longrightarrow \mathbb{R}$:

$$F(\xi, \eta)=\sum_{i=1}^{N}\varphi_i(\xi)\varphi_i(\eta), \qquad \xi, \eta \in S^{n-1}$$

は $(H_l(S^{n-1}), \langle\ ,\ \rangle)$ の正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ のとり方によらず(§11，命題3参照)，S^{n-1} によって‘内在的(intrinsic)’に定まる．したがって

$$(13) \qquad P_{l,n}(t)=\frac{a_{n-1}}{N}F(\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n, \varepsilon_n)$$

によって $P_{l,n}(t)$ を定義してももちろんかまわない．(13) は中学生にはわからないが[2)]，大学1，2年向きといえよう．(注意終)

2）(13) をわかる中学生があったらごめんなさい．

もう１つ，次の命題も成人向けである．

命題 4 $P_{l,n}(\langle\xi,\eta\rangle)=\dfrac{a_{n-1}}{N}F(\xi,\eta),\qquad \xi,\eta\in S^{n-1}.$ [3)]

証明 ξ,η が与えられたとき，まず $\sigma\eta=\varepsilon_n$ なる $\sigma\in O(\mathbb{R}^n)$ をとり，次に $\tau\in O(\mathbb{R}^{n-1})$ により

$$\tau\sigma\xi=\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n$$

とする．§11 の命題 2 から

$$(14)\qquad F(\xi,\eta)=F(\sigma\xi,\sigma\eta)=F(\sigma\xi,\varepsilon_n)=F(\tau\sigma\xi,\tau\varepsilon_n)$$
$$=F(\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n,\varepsilon_n)=\frac{N}{a_{n-1}}P_{l,n}(t)$$

ここで最後の等式は (13) による．一方，内積の不変性により

$$(15)\qquad \langle\xi,\eta\rangle=\langle\tau\sigma\xi,\tau\sigma\eta\rangle=\langle\sqrt{1-t^2}\,\varepsilon_{n-1}+t\varepsilon_n,\varepsilon_n\rangle=t.$$

(15) を (14) に代入すればよい，Q.E.D.

---

§13．直交多項式系

まずルジャンドル多項式から離れて，直交多項式系についての一般的考察から始める．$l\geqq 0$ を整数として各 l に対して l 次の多項式 $Q_l(t)\in\mathbb{R}[t]$ ($Q_0\neq 0$ する)が与えられているとする．さらに，実数の開区間 (a,b), $a<b$, で正の連続関数 $\omega(t)>0$, $t\in(a,b)$, が与えられているとする[4)]．系 $\{Q_l(t)\}$ が次の性質 (1) をもつとき重さ ω に関する**直交多項式系**とよぶ：

3） 命題 4 の等式によって $P_{l,n}(t)$ を定義しようというアイデアは魅力的であるが，右辺が $t=\langle\xi,\eta\rangle$ のみの関数であることがわかっても，それが t についての l 次の多項式であることは自明ではない．

4） $a=-\infty$，$b=+\infty$ の場合も許す．いずれの場合も，任意の整数 $k\geqq 0$ に対して積分 $\int_a^b\omega(t)t^k dt$ の有限性を仮定しておく．

(1) $$(Q_l, Q_m) = \int_a^b \omega(t) Q_l(t) Q_m(t) dt = 0, \qquad l \neq m.$$

注意1　f, g を $\mathbb{R}[t]$ の任意の多項式とするとき，ω に関する内積を

$$(f, g) = \int_a^b \omega(t) f(t) g(t) dt$$

で定める．(1) はこの内積に関する直交条件であることはいうまでもない．(注意終)

命題1　$\{Q_l(t)\}$ が直交多項式系のとき

$$(Q_l, t^m) = 0, \qquad l > m.$$

証明　$\{Q_0, Q_1, \cdots, Q_m\}$ と $\{1, t, t^2, \cdots, t^m\}$ は Q_l が l 次なことから同じベクトル空間($\mathbb{R}[t]$ の $(m+1)$ 次の部分空間)を張る．したがって $(Q_l, Q_m) = 0,\ l > m$, より $(Q_l, t^m) = 0,\ l > m$, が出る，Q.E.D.

命題2　$\{Q_l(t), \{R_l(t)\}$ がともに ω に関する直交多項式系であれば，各 $l \geqq 0$ に対して定数 $\gamma_l \neq 0$ があって

$$R_l = \gamma_l Q_l$$

が成り立つ[5]．

証明　l についての帰納法．

$l = 0$ ならば R_0, Q_0 は 0 でない定数だから，$\gamma_0 = R_0 Q_0^{-1}$ とすればよい．$l-1$ まで命題を仮定する．Q_l は l 次だから

(2) $$Q_l = \sum_{\nu=0}^{l-1} a_\nu Q_\nu + a_l t^l, \qquad a_l \neq 0$$

と書くことができる．$m < l$ ならば

$$0 = (Q_m, Q_l) = \sum_{\nu=0}^{l-1} a_\nu (Q_m, Q_\nu) + a_l (Q_m, t^l)$$
$$= a_n (Q_m, Q_m) + a_l (Q_m, t^l).$$

$(Q_m, Q_m) > 0$ に注意すれば

5）　すなわち，重さ ω (したがってその定義区間 (a, b)) が与えられれば，直交多項式系は本質的に1つしかないことを示している．

(3) $$a_m = -a_l\frac{(Q_m, t^l)}{(Q_m, Q_m)}, \qquad 0 \leqq m \leqq l-1$$

を得る．全く同様に，

(4) $$R_l = \sum_{\nu=0}^{l-1} b_\nu R_\nu + b_l t^l, \qquad b_l \neq 0$$

と書くと

(5) $$b_m = -b_l\frac{(R_m, t^l)}{(R_m, R_m)}, \qquad 0 \leqq m \leqq l-1$$

を得る．帰納法の仮定によって

(6) $$R_\nu = \gamma_\nu Q_\nu, \qquad 0 \leqq \nu \leqq l-1$$

だから，(3), (5) より

(7) $$b_\nu = -b_l\frac{(\gamma_\nu Q_\nu, t^l)}{(\gamma_\nu Q_\nu, \gamma_\nu Q_\nu)} = -\frac{b_l}{\gamma_\nu}\frac{(Q_\nu, t^l)}{(Q_\nu, Q_\nu)} = \frac{b_l}{\gamma_\nu}\frac{a_\nu}{a_l}.$$

(7) を (4) に代入して (2), (6) を用いると，

(8) $$\begin{aligned} R_l &= \sum_{\nu=0}^{l-1} b_\nu R_\nu + b_l t^l \\ &= \sum_{\nu=0}^{l-1} \frac{b_l}{\gamma_\nu}\frac{a_\nu}{a_l}\gamma_\nu Q_\nu + \frac{b_l}{a_l}a_l t^l \\ &= \frac{b_l}{a_l}\left(\sum_{\nu=0}^{l-1} a_\nu Q_\nu + a_l t^l\right) = \frac{b_l}{a_l}Q_l. \end{aligned}$$

したがって，$\gamma_l = b_l/a_l$ とおけば，(8) から $R_l = \gamma_l Q_l$ となり帰納法が完成する，Q.E.D.

命題 3　$\{Q_l(t)\}, \{R_l(t)\}$ がともに ω に関する直交多項式系で，各 $l \geqq 0$ に対して $Q_l(1) = R_l(1)$ であれば，

$$Q_l(t) = R_l(t)$$

が各 $l \geqq 0$ に対して成り立つ．すなわち 2 つの直交多項式系は全く一致する．

証明　各 $l \geqq 0$ に対して命題 2 により $R_l = \gamma_l Q_l$ となるが，両辺に $t = 1$ を代入すれば，$\gamma_l = 1$ となる，Q.E.D.

さて，ルジャンドル多項式 $P_{l,n}(t)$ にもどって，

定理 1　$n \geqq 2$ を固定したとき，$\{P_{l,n}(t)\}$ は重さ

$$\omega(t) = (1-t^2)^{(n-3)/2}, \qquad t \in (-1,1)$$

に関して直交多項式系を成す．

証明　証明すべきことは

$$(9) \qquad (P_{l,n}, P_{m,n}) = \int_{-1}^{1} P_{l,n}(t) P_{m,n}(t)(1-t^2)^{(n-3)/2} dt = 0, \qquad l \neq m$$

である．$H_l(S^{n-1})$ の正規直交底を

$$\{\varphi_1, \cdots, \varphi_N\}, \qquad N = \dim H_l(S^{n-1}),$$

$H_m(S^{n-1})$ の正規直交底を

$$\{\psi_1, \cdots, \psi_M\}, \qquad M = \dim H_m(S^{n-1})$$

とする．§10 の命題 2 から

$$(10) \qquad \langle \varphi_i, \psi_j \rangle = 0, \qquad 1 \leqq i \leqq N,\ 1 \leqq j \leqq M$$

である．命題 4 と F の定義から

$$(11) \qquad \begin{cases} P_{l,n}(\langle \xi, \varepsilon_n \rangle) = \dfrac{a_{n-1}}{N} \displaystyle\sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\varepsilon_n), \\ \\ P_{m,n}(\langle \xi, \varepsilon_n \rangle) = \dfrac{a_{n-1}}{M} \displaystyle\sum_{j=1}^{M} \psi_j(\xi)\psi_j(\varepsilon_n). \end{cases}$$

したがって，(10) により

$$(12) \qquad \int_{S^{n-1}} P_{l,n}(\langle \xi, \varepsilon_n \rangle) P_{m,n}(\langle \xi, \varepsilon_n \rangle) d\xi$$

$$= \frac{{a_{n-1}}^2}{NM} \sum_{i,j} \varphi_i(\varepsilon_n)\psi_j(\varepsilon_n)\langle \varphi_i, \psi_j \rangle = 0.$$

一方，S^{n-1} 上の積分を t を固定して得た球面 S_t^{n-2} 上の積分と t に関する区間 $(-1,1)$ 上の積分に分解する．ξ, ζ_t を S^{n-1}, S_t^{n-2} の一般点として微分(面積要素) $d\xi$ を分解すると，図 9 からわかるように，

$$(13) \qquad d\xi = d\zeta_t \cdot \frac{dt}{\sqrt{1-t^2}}$$

となる．さらに S_t^{n-2} は S^{n-2} (赤道) を $\sqrt{1-t^2}$ の割合で縮小したものであるか

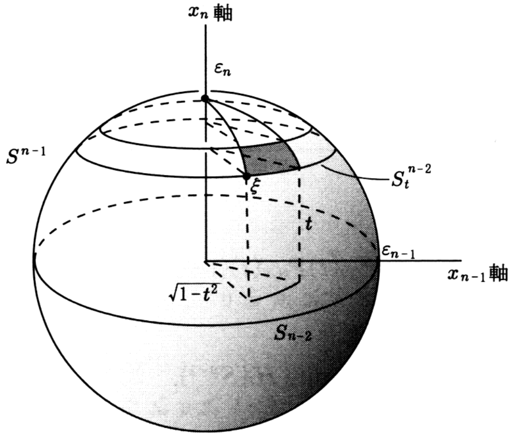


図 9

ら

(14) $\quad d\zeta_t = (1-t^2)^{(n-2)/2} d\zeta$

である．したがって $t = \langle \xi, \varepsilon_n \rangle$ に注意すれば，(12) の積分に (13), (14) を用いて

(15) $$\int_{S^{n-1}} P_{l,n}(\langle \xi, \varepsilon_n \rangle) P_{m,n}(\langle \xi, \varepsilon_n \rangle) d\xi$$

$$= a_{n-2} \int_{-1}^{1} P_{l,n}(t) P_{m,n}(t)(1-t^2)^{(n-3)/2} dt$$

を得る．そして，(15) を (12) に代入して (9) を得る，Q.E.D.

ここで，以下しばしば用いる記号を導入する．それは階乗 $n!$ の拡張である．

定義 1 $\alpha \in \mathbb{C}$, $n \geqq 0$ (整数) に対して

$$(\alpha)_0 = 1,$$

$$(\alpha)_n = \alpha(\alpha+1)\cdots(\alpha+n-1), \qquad n \geqq 1$$

とおく[6]．

定理 2　$n \geqq 2, l \geqq 0$ のとき

$$P_{l,n}(t) = \frac{(-1)^l}{2^l\left(\dfrac{n-1}{2}\right)_l}(1-t^2)^{(3-n)/2}\left(\frac{d}{dt}\right)^l(1-t^2)^{l+(n-3)/2}$$

が成り立つ.

注意 2　証明する前に定理 2 の意味を説明する. $n=3$ とすると

$$\left(\frac{n-1}{2}\right)_l = (1)_l = l!$$

となる. また, $(1-t^2)^l$ を $(t^2-1)^l$ と書き換えるとちょうど $(-1)^l$ が出る. したがって

$$(16) \qquad P_{l,3}(t) = \frac{1}{2^l l!}\left(\frac{d}{dt}\right)^l(t^2-1)^l$$

となり, §1 の式 (11) の $P_l(t)$ (ルジャンドルの意味のルジャンドル多項式)と一致する. これによって, 我々の定義した $P_{l,n}(t)$, $n \geqq 2$, は古典的なルジャンドル多項式の自然な拡張であり, 我々がすでにやってきたように, $P_{l,n}(t)$ を単にルジャンドル多項式と呼ぶことは全く合理的であることが確立したのである. (注意終)

定理 2 の証明は命題 3 によるので, 定理 2 の両辺の関数の $t=1$ における値を定めておく.

補題 1　$P_{l,n}(1) = 1$.

補題 1 の証明　§12 の定義 2 より

$$P_{l,n}(1) = c_0 = 1, \qquad \text{Q.E.D.}$$

補題 2　定理 2 の右辺の t の関数を $R_l(t)$ とおくと

$$R_l(1) = 1$$

である.

6)　$n! = (1)_n$ と書くことができる.

補題 2 の証明

$$\varphi_l(t)=(1-t^2)^{-r}\left(\frac{d}{dt}\right)^l(1-t^2)^{l+r},\qquad r=\frac{n-3}{2}$$

とおく.

$$(17)\qquad R_l(t)=\frac{(-1)^l}{2^l\left(\frac{n-1}{2}\right)_l}\varphi_l(t)$$

だから,

$$(18)\qquad \varphi_l(1)=(-1)^l\cdot 2^l\left(\frac{n-1}{2}\right)_l$$

を確かめればよい. 実際,

$$\begin{aligned}\varphi_l(t)&=(1-t)^{-r}(1+t)^{-r}\left(\frac{d}{dt}\right)^l((1-t)^{l+r}(1+t)^{l+r})\\&=(1-t)^{-r}(1+t)^{-r}\sum_{\nu=0}^{l}\binom{l}{\nu}\left(\frac{d}{dt}\right)^\nu(1-t)^{l+r}\left(\frac{d}{dt}\right)^{l-\nu}(1+t)^{l+r}\\&=(1-t)^{-r}(1+t)^{-r}\sum_{\nu=0}^{l}\Bigg\{\binom{l}{\nu}(-1)^\nu(l+r)\cdots(l+r-\nu+1)\\&\qquad\times(1-t)^{l+r-\nu}(l+r)\cdots(l+r-l+\nu+1)\\&\qquad\times(1+t)^{l+r-l+\nu}\Bigg\}\\&=\sum_{\nu=0}^{l}\Bigg\{\binom{l}{\nu}(-1)^\nu(l-r)\cdots(l+r-\nu+1)(1-t)^{l-\nu}\\&\qquad\times(l+r)\cdots(r+\nu+1)(1+t)^\nu\Bigg\}.\end{aligned}$$

ここで, $t=1$ とおくと, 上の和で $\nu=l$ の項だけが生き残るから

$$\varphi_l(1)=(-1)^l(r+1)\cdots(r+l)\cdot 2^l=(-1)^l\cdot 2^l\left(\frac{n-1}{2}\right)_l$$

となり, (18) が確かめられた, Q.E.D.

定理 2 の証明　補題 1，補題 2 により，$\{\varphi_l(t)\}$ が

$$\omega(t)=(1-t^2)^r, \qquad r=\frac{n-3}{2}, \quad t\in(-1,1)$$

に関する直交関数系であることを証明すれば定理 2 は命題 3 に帰する．まず $\varphi_l(t)$ が t の l 次の多項式であることは容易にわかる．したがって

$$\int_{-1}^{1}t^k\varphi_l(t)(1-t^2)^r dt=0, \qquad k<l \tag{19}$$

がいえれば十分である．さて，(19) の左辺を計算すると，

$$\begin{aligned}
&\int_{-1}^{1}t^k(1-t^2)^{-r}\left(\left(\frac{d}{dt}\right)^l(1-t^2)^{l+r}\right)(1-t^2)^r dt \\
&=\int_{-1}^{1}t^k\left(\frac{d}{dt}\right)^l(1-t^2)^{l+r}dt \qquad (\text{部分積分}) \\
&=\left[t^k\left(\frac{d}{dt}\right)^{l-1}(1-t^2)^{l+r}\right]_{-1}^{1}-k\int_{-1}^{1}t^{k-1}\left(\frac{d}{dt}\right)^{l-1}(1-t^2)^{l+r}dt.
\end{aligned} \tag{20}$$

ここで最初の項は 0 になる．後の必要のためにやや一般の関係

$$\left[t^{k-\mu}\left(\frac{d}{dt}\right)^{l-\mu-1}(1-t^2)^{l+r}\right]_{-1}^{1}=0, \qquad 0\leqq\mu\leqq k \tag{21}$$

を注意しておく．実際，

$$\begin{aligned}
&\left(\frac{d}{dt}\right)^{l-\mu-1}(1-t)^{l+r}(1+t)^{l+r} \\
&=\sum_{\nu=0}^{l-\mu-1}\left\{\binom{l-\mu-1}{\nu}\left(\frac{d}{dt}\right)^{\nu}(1-t)^{l+r}\left(\frac{d}{dt}\right)^{l-\mu-1-\nu}(1+t)^{l+r}\right\} \\
&=\sum_{\nu=0}^{l-\mu-1}\left\{\binom{l-\mu-1}{\nu}(l+r)\cdots(l+r-\nu+1)(1-t)^{l+r-\nu}\right. \\
&\qquad \left.\times(l+r)\cdots(l+r-l+\mu+1+\nu+1)(1+t)^{l+r-l+\mu+1+\nu}\right\}
\end{aligned}$$

となり，指数 $l+r-\nu$, $l+r-l+\mu+1+\nu$ がどの ν についても決して 0 にならないことから (21) が出る．

とくに (21) で $\mu=0$ とおいて，(20) は

$$(22)\qquad \int_{-1}^{1} t^k\left(\frac{d}{dt}\right)^l (1-t^2)^{l+r}dt = -k\int_{-1}^{1} t^{k-1}\left(\frac{d}{dt}\right)^{l-1}(1-t^2)^{l+r}dt$$

を与える．以下 (21) を順々に用いると，結局

$$(23)\qquad \int_{-1}^{1} t^k\left(\frac{d}{dt}\right)^l (1-t^2)^{l+r}dt = (-1)^k k!\left[\left(\frac{d}{dt}\right)^{l-k-1}(1-t^2)^{l+r}\right]_{-1}^{1} = 0$$

に到達する，(定理 2 の)Q.E.D.

次の定理 3 を証明する前に補題を 1 つやっておく．

補題 3　$u_1, \cdots, u_r$, $r \leqq N$, を $H_l(S^{n-1})$ の 1 次独立な関数とすると，S^{n-1} の r 個の点 $\eta_1, \cdots, \eta_r$ を選んで

$$\det(u_i(\eta_j)) \neq 0$$

にすることができる．

補題 3 の証明　$u_1 \neq 0$ だから $\eta_1 \in S^{n-1}$ で $u_1(\eta_1) \neq 0$ なるものがある[7)]．次に $\xi \in S^{n-1}$ として，

$$\begin{vmatrix} u_1(\eta_1) & u_1(\xi) \\ u_2(\eta_1) & u_2(\xi) \end{vmatrix} = 0$$

がすべての $\xi \in S^{n-1}$ について成り立ったとすると

$$u_2(\xi) = \frac{u_2(\eta_1)}{u_1(\eta_1)} u_1(\xi)$$

となり，u_1, u_2 が独立なことに矛盾する．したがって，

$$(24)\qquad \begin{vmatrix} u_1(\eta_1) & u_1(\eta_2) \\ u_2(\eta_1) & u_2(\eta_2) \end{vmatrix} \neq 0$$

なる $\eta_2 \in S^{n-1}$ がとれる．次に，$\xi \in S^{n-1}$ として

$$\begin{vmatrix} u_1(\eta_1) & u_1(\eta_2) & u_1(\xi) \\ u_2(\eta_1) & u_2(\eta_2) & u_2(\xi) \\ u_3(\eta_1) & u_3(\eta_2) & u_3(\xi) \end{vmatrix} = 0$$

がすべての $\xi \in S^{n-1}$ について成り立ったとすると，(24) を用いて u_3 が u_1,

7）　同型 $H_l(\mathbb{R}^n) \approx H_l(S^{n-1})$ で u_1 を斉次多項式と見れば，$\eta_1 \in \mathbb{R}^n$ で $u_1(\eta_1) \neq 0$ なるものがある．u_1 の斉次性から $\eta_1 \in S^{n-1}$ としてよい．以下同様である．

u_2 の1次結合となり，u_1, u_2, u_3 が独立なことに矛盾する．以下同様，Q.E.D.

定理 3(展開定理)　$H_l(S^{n-1})$ の正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ に対して，補題3により $\eta_1, \cdots, \eta_N \in S^{n-1}$ を

$$\det(\varphi_i(\eta_j)) \neq 0$$

となるようにとると，任意の $\varphi \in H_l(S^{n-1})$ は

$$\varphi(\xi) = \sum_{j=1}^{N} c_j P_{l,n}(\langle \xi, \eta_j \rangle), \qquad c_j \in \mathbb{R}$$

と一意的にあらわされる．

証明　§12の命題4により

$$(25) \qquad P_{l,n}(\langle \xi, \eta_j \rangle) = \frac{a_{n-1}}{N} F(\xi, \eta_j) = \frac{a_{n-1}}{N} \sum_{i=1}^{N} \varphi_i(\xi) \varphi_i(\eta_j).$$

ここで $\det(\varphi_i(\eta_j)) \neq 0$ により (25) を φ_i について解けば，

$$(26) \qquad \varphi_i(\xi) = \sum_{i=1}^{N} c_{ij} P_{l,n}(\langle \xi, \eta_j \rangle)$$

と書ける．これから明らかに任意の $\varphi \in H_l(S^{n-1})$ は定理3に述べたように書ける．一意性は明らかである，Q.E.D.

§14．$n=2$ の場合

§8の定理2によれば

$$(1) \qquad h_l(n) = \dim H_l(S^{n-1}) = \binom{n+l-1}{l} - \binom{n+l-3}{l-2}$$

であったから，(1) で $n=2$ とおいて

$$(2) \qquad h_l(2) = (l+1) - (l-1) = 2, \qquad l \geqq 1$$

が成り立つ[8)]．

さて，S^1 上の点 ξ は図 10 のように角 θ と対応するから ξ と θ を同一視し，

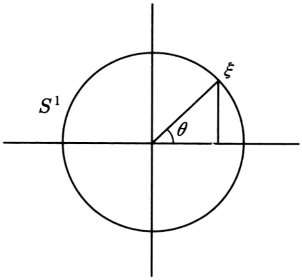


図 10

$$\varphi_1(\xi) = \frac{1}{\sqrt{\pi}} \cos l\theta, \qquad \varphi_2(\xi) = \frac{1}{\sqrt{\pi}} \sin l\theta$$

とおく．$\varphi_i \in H_l(S^1)$ である．実際，

$$\begin{aligned} f(x) &= \mathrm{Re}(x_1 + ix_2)^l, \\ g(x) &= \mathrm{Im}(x_1 + ix_2)^l \end{aligned} \qquad x = (x_1, x_2) \in \mathbb{R}^2$$

とおけば，f, g は複素解析関数 $(x_1+ix_2)^l$ の実部および虚部であるから調和関数である．すなわち $f, g \in H_l(\mathbb{R}^2)$.

さて

$$(x_1 + ix_2)^l = r^l(\cos\theta + i\sin\theta)^l = r^l(\cos l\theta + i\sin l\theta)$$

だから

$$f(\xi) = \sqrt{\pi}\varphi_1(\xi), \qquad g(\xi) = \sqrt{\pi}\varphi_2(\xi)$$

となり $\varphi_i \in H_l(S^1)$ が出た．次に

$$\langle \varphi_1, \varphi_1 \rangle = \frac{1}{\pi}\int_0^{2\pi} \cos^2 l\theta d\theta = 1,$$

$$\langle \varphi_2, \varphi_2 \rangle = \frac{1}{\pi}\int_0^{2\pi} \sin^2 l\theta d\theta = 1,$$

8） $l=0$ のときは $h_0(2)=1$ であることはいうまでもない．以下，この場合は除外する．

$$\langle \varphi_1, \varphi_2 \rangle = \frac{1}{\pi}\int_0^{2\pi} \cos l\theta \cdot \sin l\theta d\theta = 0$$

であるから $\{\varphi_1, \varphi_2\}$ は $H_l(S^1)$ の正規直交底になる．次に

$$\eta_1 = (1, 0), \qquad \eta_2 = \left(\cos\frac{\pi}{2l}, \sin\frac{\pi}{2l}\right)$$

なる 2 点を S^1 からとる．まず

$$\pi\begin{vmatrix} \varphi_1(\eta_1) & \varphi_1(\eta_2) \\ \varphi_2(\eta_1) & \varphi_2(\eta_2) \end{vmatrix} = \begin{vmatrix} 1 & \cos\dfrac{\pi}{2} \\ 0 & \sin\dfrac{\pi}{2} \end{vmatrix} = 1 \neq 0.$$

次に，

$$\begin{aligned} P_{l,2}(\langle \xi, \eta_1 \rangle) &= \pi(\varphi_1(\xi)\varphi_1(\eta_1) + \varphi_2(\xi)\varphi_2(\eta_1)) \\ &= \cos l\theta \cdot 1 + \sin l\xi \cdot 0 = \cos l\theta, \\ P_{l,2}(\langle \xi, \eta_2 \rangle) &= \pi(\varphi_1(\xi)\varphi_1(\eta_2) + \varphi_2(\xi)\varphi_2(\eta_2)) \\ &= \cos l\theta \cdot \cos\frac{\pi}{2} + \sin l\theta \cdot \sin\frac{\pi}{2} = \sin l\theta. \end{aligned}$$

したがって，§13 の定理 3 による $\varphi \in H_l(S^1)$ の展開は

(3)　$\varphi(\theta) = c_1 \cos l\theta + c_2 \sin l\theta$

に他ならない．直交直和分解

(4)　$P(S^1) = \bigoplus_{l=0}^{\infty} H_l(S^1)$

を用いれば，(3) から任意の $\varphi \in P(S^1)$ のフーリエ展開が得られる．

最後に $P_{l,2}(t)$ を求めてみよう：

$$\begin{aligned} P_{l,2}(t) &= \pi(\varphi_1\sqrt{1-t^2}\,\varepsilon_1 + t\varepsilon_2)\varphi_1(\varepsilon_2) + \varphi_2(\sqrt{1-t^2}\,\varepsilon_1 + t\varepsilon_2)\varphi_2(\varepsilon_2)) \\ &= \cos l\psi \cdot \cos l\frac{\pi}{2} + \sin l\psi \cdot \sin l\frac{\pi}{2} \\ &= \cos l\left(\psi - \frac{\pi}{2}\right) = \cos l\left(\frac{\pi}{2} - \psi\right) = \cos(l \cos^{-1} t). \end{aligned}$$

いい換えれば，$P_{l,2}(t)$ は

(5)　$P_{l,2}(\cos\theta) = \cos l\theta, \qquad l \geqq 0$

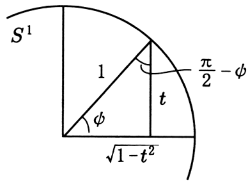


図 11

で定まる．この $P_{l,2}$ は通常チェビシェフの多項式とよばれている．(5) は要するに $\cos l\theta$ は $\cos\theta$ の多項式であるというだけのことである．

$n=3$ が古典的の場合である．次回は，§1 の(10)に予告した $H_l(S^2)$ の $2l+1$ 個の底

$$\begin{cases} P_l(\cos\theta), \\ \cos m\varphi\cdot\sin^m\theta\, P_l^{(m)}(\cos\theta), \qquad 1\leqq m\leqq l \\ \sin m\varphi\cdot\sin^m\theta\, P_l^{(m)}(\cos\theta) \end{cases}$$

がどのようにして得られるかを解説する．ここで

$$P_l(t)=P_{l,3}(t)$$

である．

第6回

ラプラス方程式
反省

前回，任意の $n \geqq 2$ と $l \geqq 0$ に対してルジャンドル多項式 $P_{l,n}(t)$ を定義し，n を固定したとき $\{P_{l,n}(t)\}$ が直交多項式系をなし，それを用いて我々の定義(帯球関数の空間 $Z_l(S^{n-1})$ に基づくもの；§12，定義2，命題3)と古典的な高階微分による定義(§13，定理2)とが一致することを確かめました．

今回は，まず $n=3$ として，§1の式 (10) で予告した $H_l(S^2)$ の $2l+1$ 個の底がどのようにして得られるかを説明しましょう．これは全く古典的な話題ですが，こうすることにより，豊かな多面性を持つルジャンドル多項式の今まで見過ごしていたいくつかの側面に自然に導かれます．

§15．ラプラス方程式

この節ではずっと $n=3$ だから，

(1) $$P_l(t)=P_{l,3}(t), \qquad l \geqq 0$$

と略記する．§13の定理2で $n=3$ とすると

(2) $$P_l(t)=\frac{1}{2^l l!}\left(\frac{d}{dt}\right)^l (t^2-1)^l$$

になる．さらに，整数 $m \geqq 0$ に対して

(3) $$P_l^{(m)}(t) = \left(\frac{d}{dt}\right)^m P_l(t)$$

とおく[1]. $P_l(t)$ は l 次だから，$0 \leqq m \leqq l$ で十分である.

命題 1(微分方程式) $P_l^{(m)}(t)$ は 2 階線型微分方程式：

$$(1-t^2)y''-2(m+1)ty'+(l(l+1)-m(m+1))y = 0$$

を満足する.

証明 $u = (t^2-1)^l$ とおくと $u' = l(t^2-1)^{l-1}\cdot 2t$. したがって

(4) $$(t^2-1)u' = 2lt(t^2-1)^l = 2ltu.$$

(4) の両端の式を $l+1$ 回微分すると

(5) $$\sum_{k=0}^{l+1}\binom{l+1}{k}(t^2-1)^{(k)}u^{(l+2-k)} = 2l\sum_{k=0}^{l+1}\binom{l+1}{k}t^{(k)}u^{(l+1-k)}.$$

この (5) の左辺は $k = 0, 1, 2,$ まで，右辺は $k = 0, 1$ まで生き残るから，

(6) $$(t^2-1)u^{(l+2)}+2(l+1)tu^{(l+1)}+l(l+1)u^{(l)} = 2ltu^{(l+1)}+2l(l+1)u^{(l)},$$

すなわち，

(7) $$(t^2-1)u^{(l+2)}+2tu^{(l+1)}-l(l+1)u^{(l)} = 0.$$

いいかえれば，(7) より，

(8) $$(1-t^2)P_l''-2tP_l'+l(l+1)P_l = 0.$$ [2]

さて，(8) を次々と微分していくと：

$$(1-t^2)P_l'''-2(2t)P_l''+(l(l+1)-1\cdot 2)P_l' = 0,$$

$$(1-t^2)P_l''''-3(2t)P_l'''+(l(l+1)-2\cdot 3)P_l'' = 0,$$

$$\cdots\cdots\cdots\cdots\cdots$$

$$(1-t^2)P_l^{(m+2)}-(m+1)(2t)P_l^{(m+1)} +(l(l+1)-m(n+1))P_l^{(m)} = 0,$$ Q.E.D.

---

1) 一般に $y = f(x)$ の第 m 導関数を

$$y^{(m)} = f^{(m)}(x)$$

と書く.

2) $P_l(t) = \frac{1}{2^l l!}u^{(l)}$ に注意. (8) は $P_l(t)$ 自身の微分方程式である.

命題 2（直交性）

$$\int_{-1}^{1}(1-t^2)^m P_l^{(m)}(t)P_k^{(m)}(t)dt = 0, \qquad l \neq k.$$ [3]

証明　命題1を $P_l^{(m)}$ と $P_k^{(m)}$ に用いて

$$(9)\qquad \begin{cases} (1-t^2)P_l^{(m+2)}-2(m+1)tP_l^{(m+1)} \\ \qquad\qquad +(l(l+1)-m(m+1))P_l^{(m)}=0, \\ (1-t^2)P_k^{(m+2)}-2(m+1)tP_k^{(m+1)} \\ \qquad\qquad +(k(k+1)-m(m+1)P_k^{(m)}=0. \end{cases}$$

(9) の第1式に $(1-t^2)^m P_k^{(m)}$，第2式に $(1-t^2)P_l^{(m)}$ を掛けて引き算をすると

$$(10)\qquad \begin{aligned} &(1-t^2)^{m+1}(P_l^{(m+2)}P_k^{(m)}-P_k^{(m+2)}P_l^{(m)}) \\ &\quad -2(m+1)t(1-t^2)^m(P_l^{(m+1)}P_k^{(m)}-P_k^{(m+1)}P_l^{(m)}) \\ &\quad\quad =(k(k+1)-l(l+1))(1-t^2)^m P_l^{(m)}P_k^{(m)}. \end{aligned}$$

いま，

$$(11)\qquad u=P_l^{(m+1)}P_k^{(m)}-P_k^{(m+1)}P_l^{(m)}$$

とおけば

$$(12)\qquad u'=P_l^{(m+2)}P_k^{(m)}-P_k^{(m+2)}P_l^{(m)}$$

となるから，(10) を

$$(13)\qquad ((1-t^2)^{m+1}u)'=(k(k+1)-l(l+1))(1-t^2)^m P_l^{(m)}P_k^{(m)}$$

と書くことができる．(13) を区間 $(-1,1)$ で積分して

$$(k(k+1)-l(l+1))\int_{-1}^{1}(1-t^2)^m P_l^{(m)}P_k^{(m)}dt$$

$$=\Big[(1-t^2)^{m+1}u\Big]_{-1}^{1}=0,$$

$k\neq l$ ならば $k(k+1)-l(l+1)\neq 0$ だから

$$\int_{-1}^{1}(1-t^2)^m P_l^{(m)}P_k^{(m)}dt=0, \qquad \text{Q.E.D.}$$

さて，ここで，あまりにも有名な問題であるが，ラプラス方程式

3）　$m=0$ のときは既知である（§13，定理1）．ここでは命題1の応用として出してみた．

$$(14)\qquad \Delta V=\left(\left(\frac{\partial}{\partial x_1}\right)^2+\left(\frac{\partial}{\partial x_2}\right)^2+\left(\frac{\partial}{\partial x_3}\right)^2\right)V=0$$

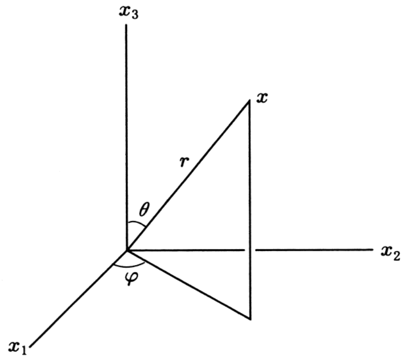


図 12

を極座標 (r, θ, φ) について解くことを復習してみよう．これはルジャンドル多項式の最も大切な応用例であって，ガウスの相互律に対するガウスの和の役割りに相当すると思う．仕上がったクロスワード・パズルで書けば，

	数論	解析
道具	ガウスの和	ルジャンドル多項式
応用	相互律	ラプラス方程式

となるでしょう．いうまでもなく極座標と直交座標は

$$(15)\qquad \begin{cases} x_1 = r\sin\theta\cos\varphi, \\ x_2 = r\sin\theta\sin\varphi, \\ x_3 = r\cos\theta \end{cases}$$

で結ばれている．ラプラス方程式を (r, θ, φ) についての方程式に書き直すことは，言うは易しいが，実行するのはかなり忍耐がいる[4)]．私も 1 回だけやっ

4） Every student of mathematics should carry out the necessary calculations at least once in his life, but perhaps once is enough! (G. Simmons, 《Differential Equations》 McGraw-Hill, 1972, p.251)

てみた．結果は，

(16)　$$\Delta V=\frac{\partial}{\partial r}\left(r^2\frac{\partial V}{\partial r}\right)+\frac{1}{\sin\theta}\cdot\frac{\partial}{\partial\theta}\left(\sin\theta\frac{\partial u}{\partial\theta}\right)+\frac{1}{\sin^2\theta}\left(\frac{\partial}{\partial\varphi}\right)^2V=0$$

となる．以下ホブソンの本(E. W. Hobson,《The theory of spherical and ellipsoidal harmonics》Chelsea, 1965, p.9-p.10)に従って (16) を解いてみる．そこで

(17)　$$V=R\Theta\Phi$$

で R,Θ,Φ はそれぞれ r,θ,φ のみの 1 変数関数となっている場合を考える．(17) を (16) に入れて $V=R\Theta\Phi$ で割ると

(18)　$$\frac{1}{R}\frac{d}{dr}\left(r^2\frac{dR}{dr}\right)+\frac{1}{\Theta\sin\theta}\frac{d}{d\theta}\left(\sin\theta\frac{d\Theta}{d\theta}\right)+\frac{1}{\Phi\sin^2\theta}\left(\frac{d}{d\varphi}\right)^2\Phi=0.$$

さて，整数 $l\geqq 0$ に対して

(19)　$$\frac{1}{R}\frac{d}{cr}\left(r^2\frac{dR}{dr}\right)=l(l+1)$$

は

(20)　$$R=r^l$$

なる解をもつ．(19) を (18) に入れ，$\sin^2\theta$ を掛ければ，

(21)　$$l(l+1)\sin^2\theta+\frac{\sin\theta}{\Theta}\frac{d}{d\theta}\left(\sin\theta\frac{d\Theta}{d\theta}\right)+\frac{\Phi''}{\Phi}=0$$

となる．ここで整数 $m\geqq 0$ に対して

(22)　$$\Phi=A_m\cos m\varphi+B_m\sin m\varphi,\qquad A_m,B_m\in\mathbb{R}$$

とおくと

(23)　$$\frac{\Phi''}{\Phi}=-m^2$$

になるから，(21) に Θ を掛けて $\sin^2\theta$ で割れば

(24)　$$\frac{1}{\sin\theta}\frac{d}{d\theta}\left(\sin\theta\frac{d\Theta}{d\theta}\right)-\left(l(l+1)-\frac{m^2}{\sin^2\theta}\right)\Theta=0$$

になる．そこで

(25)　$$\cos\theta=t,\qquad \Theta=u$$

と書き換えれば，(24) は

$$(26)\qquad \frac{d}{dt}\left((1-t^2)\frac{du}{dt}\right)+\left(l(l+1)-\frac{m^2}{1-t^2}\right)u=0$$

となる．(26) を変形すると

$$(27)\qquad (1-t^2)u''-2tu'+\left(l(l+1)-\frac{m^2}{1-t^2}\right)u=0.$$

そこで変数変換

$$(28)\qquad u=(1-t^2)^{m/2}v$$

を行うと，(27) は

$$(29)\qquad (1-t^2)v''-2(m+1)tv'+(l(l+1)-m(m+1))v=0$$

となる[5]．ところが (29) は命題 1 の微分方程式である．したがって

$$(30)\qquad v=P_l^{(m)}(t)$$

という解がある．(28) により

$$(31)\qquad u=(1-t^2)^{m/2}P_l^{(m)}(t)$$

が (27)，すなわち (26) を満足し，(25), (31) から

$$(32)\qquad \Theta=\sin^m\theta P_l^{(m)}(\cos\theta)$$

が (24) を満足する．最後に，(20), (22), (32) から

$$(33)\qquad \begin{aligned} V&=R\Theta\Phi\\ &=r^l\sin^m\theta P_l^{(m)}(\cos\theta)(A_m\cos m\varphi+B_m\sin m\varphi)\end{aligned}$$

がラプラス方程式 (14) の解であることがわかった．

以下，$x\in\mathbb{R}^3$ を極座標で考えて

$$(34)\qquad \begin{cases} f_l(x)=r^lP_l(\cos\theta),\\ f_{l,m}(x)=r^l\cos m\varphi\cdot\sin^m\theta P_l^{(m)}(\cos\theta),\\ g_{l,m}(x)=r^l\sin m\varphi\cdot\sin^m\theta P_l^{(m)}(\cos\theta), \qquad 1\leqq m\leqq l\end{cases}$$

と書くことにする．(34) の各関数は (33) から調和関数である．さらに，これらが直交座標 $x=(x_1,x_2,x_3)$ にもどしたとき多項式であることがいえる．これが次の命題である．

命題 3　(34) で定義された $2l+1$ 個の関数はいずれも $H_l(\mathbb{R}^2)$ に属する．

---

5)　(28) を (27) に入れて (29) を出すのも少し忍耐がいる．

証明　各関数が調和関数であることはすでに解っているから，それらが $P_l(\mathbb{R}^3)$ に属することをいえばよい．まず，§12の定義2から

$$P_l(t)=\sum_{l-j\equiv 0(2)} c_{l-j}t^j(1-t^2)^{(l-j)/2}, \qquad 0\leqq j\leqq l$$

と書けるから，$j\equiv l\,(2)$ で $P_l(t)$ は t の偶数巾のみまたは奇数巾のみから成る．したがって，m 回微分すれば

$$(35)\qquad P_l^{(m)}(t)=\sum_{\nu} b_\nu t^{l-m-2\nu}$$

の形をしている．次に

$$\cos m\varphi+i\sin m\varphi=(\cos\varphi+i\sin\varphi)^m$$

の両辺を比較することにより $\cos m\varphi, \sin m\varphi$ がともに

$$(36)\qquad \sum_k a_k\cos^{m-k}\varphi\sin^k\varphi$$

の形をしていることが解る．したがって，$f_l, f_{l,m}, g_{l,m}$ は

$$(37)\qquad r^l\cos^{m-k}\varphi\cdot\sin^k\varphi\cdot\sin^m\theta(\cos\theta)^{l-m-2\nu}$$

の形の項の1次結合になるが，(37) は

$$\begin{aligned}(37)&=r^{2\nu}(r^{m-k}\cos^{m-k}\varphi\cdot\sin^{m-k}\theta)\\&\quad\times(r^k\sin^k\varphi\cdot\sin^k\theta)(r^{l-m-2\nu}\cos^{l-m-2\nu}\theta)\\&=q(x)^\nu x_1{}^{m-k}x_2{}^k x_3{}^{l-m-2\nu}\in P_l(\mathbb{R}^3)\end{aligned}$$

とあらわされるから $f_l, f_{l,m}, g_{l,m}$ はすべて $\in P_l(\mathbb{R})^3$, Q.E.D.

定義1　$f_l, f_{l,m}, g_{l,m}$ を S^2 に制限して得た $H_l(S^2)$ の関数を $\varphi_l, \varphi_{l,m}, \psi_{l,m}$ と書く．

定理1　$2l+1$ 個の関数 $\varphi_l, \varphi_{l,m}, \psi_{l,m}$, $1\leqq m\leqq l$, は $H_l(S^2)$ の底になる．さらに，$H_l(S^2)$ の内積 $\langle\ ,\ \rangle$ に関してこれらの関数のどの2つも互いに直交する[6]．

6）$\{\varphi_l, \varphi_{l,m}, \psi_{l,m}\}$ は直交底であるが，一般に長さが1でないので正規直交底ではない．この定理1により§1で予告されていた (10) が証明されたわけである．

証明　$\dim H_l(S^2) = \binom{l+2}{l} - \binom{l}{l-2} = 2l+1$

だから，直交性がいえれば1次独立性が出て証明がすむ[7]．S^2 の面積要素

$$d\xi = \sin\theta d\theta d\varphi$$

に注意すれば，

$$(38)\qquad \langle \varphi_{l,m}, \varphi_{l,m'} \rangle = \int_{S^2} \varphi_{l,m}\varphi_{l,m'} d\xi = \int_0^{2\pi} d\varphi \int_0^{2\pi} \varphi_{l,m}\varphi_{l,m'} \sin\theta d\theta$$

$$= \int_0^{2\pi} \cos m\varphi \cdot \cos m'\varphi d\varphi$$

$$\times \int_0^{\pi} \sin^{m+m'+1}\theta \cdot P_l^{(m)}(\cos\theta) P_l^{(m')}(\cos\theta) d\theta.$$

$\langle \psi_{l,m}, \psi_{l,m'} \rangle$ では，(38) の最終項に相当するところで第2因子は (38) と同じで，第1因子は

$$\int_0^{2\pi} \sin m\varphi \cdot \sin m'\varphi d\varphi$$

になる．$\langle \varphi_{l,m}, \psi_{l,m'} \rangle$ でも第2因子は同じで，第1因子は

$$\int_0^{2\pi} \cos m\varphi \cdot \sin m'\varphi d\varphi$$

になる．したがって問題の直交性は，よく知られた

$$\{1, \sin\varphi, \cos\varphi, \cdots, \sin m\varphi, \cos m\varphi, \cdots\}$$

の $(0, 2\pi)$ での直交性に帰せられる，Q.E.D.

注意1　§15で，$n=3$ で述べたことの $n \geqq 4$ への拡張は P. Appell-J. Kampé de Fériet,《Fonctions hypergéometriques et hypersphériques, polynomes d'Hermite》Gauthier-Villars, Paris, 1926，に書いてある．

注意2　ガウスの超幾何級数

$$F(a, b\,; c\,; x) = \sum_{\nu=0}^{\infty} \frac{(a)_\nu (b)_\nu}{(c)_\nu} \frac{x^\nu}{\nu!}$$

を用いると，任意の $n \geqq 2$ に対して

7）どの関数も0でないことは (34) の式(で $r=1$ とおいたもの)を見れば明らか．

$$P_{l,n}(t) = F\left(-l, l+n-2; \frac{n-1}{2}; \frac{1-t}{2}\right)$$

という式が成り立つ[8]．このようにして，ルジャンドル多項式は超幾何多項式の一部分となる．超幾何多項式，より一般に超幾何関数はやはり2階線型微分方程式を満足する．$P_{l,n}(t)$ の場合は

$$(1-t^2)P''_{l,n}-(n-1)tP'_{l,n}+l(l+n-2)P_{l,n}=0$$

で，$n=3$ とおけば，命題1で $m=0$ のときの式になる．超幾何関数の満足する微分方程式はいわゆるフックス型で代数的にコントロールしやすいものである．これに関しては久賀道郎さんの『ガロアの夢』(日本評論社，1968)参照．

ついでに，本のことをいうと，§15を解析的方向に徹底させるとE. T. Whittaker - G. N. Watson,《Modern Analysis》4th ed., Cambridge, 1958, となる．

また，群論的方向に徹底させると，N. J. Vilenkin,《Special Functions and the Theory of Group Representations》Translations of Mathematical Monographs, vol. 22, A. M. S. Providence, 1968，となる．

§16．反省

今まで6回にわたって「ガウスの和とルジャンドル多項式」と題する連載を続けてまいりました．最初のお約束が6回ということでしたので，今回でやめることにします．その前にひとこと，今までやったことを用いて，ガウスの和とルジャンドル多項式に共通な論理的構造を反省してみましょう．

純粋に論理的な要求に従って次の情況を考える．

8）$(a)_\nu = a(a+1)\cdots(a+\nu-1)$,　　$(a)_0 = 1$.

$$(\#)\quad \begin{cases} K^n: \text{任意の体}\ K\ \text{上の}\ n\ \text{次元ベクトル空間}, \\ \langle x, y\rangle = x_1y_1 + \cdots + x_ny_n: K^n\ \text{の普通の内積}, \\ S: K^n\ \text{のある部分集合(図形)}, \\ \varPhi: S\ \text{上のある}\ N\ \text{次元の関数空間}^{9)}. \end{cases}$$

さて，(#) の情況のもとに次の 2 つの性質 (A), (B) をもつ関数

$$P: K \longrightarrow \mathbb{R}$$

の存在を問題とする．

> (A) $\xi, \eta \in S$ に対して
>
> $$\pi_\eta(\xi) = P(\langle \xi, \eta\rangle)$$
>
> で定まる π_η は $\varPhi$ に属する．
>
> (B) S の N 個の点からなる部分集合 E を適当に選ぶと $\{\pi_\eta\}, \eta \in E$, はベクトル空間 $\varPhi$ の底になる．

(#) や (A), (B) はいうまでもなくルジャンドル多項式 $P_{l,n}$ の理論をモデルにして，あるいは抽象化して得られたものである．念のため復習すると $P_{l,n}$ は (#), (A), (B) を下のように特殊化したものである．

$K^n = \mathbb{R}^n$: 内積 $\langle\ ,\ \rangle$ についてのユークリッド空間，

$S = S^{n-1}$: $\mathbb{R}^n$ の単位球面，

$\varPhi = H_l(S^{n-1})$: l 次の球面調和関数全体の空間，

$$N = \dim \varPhi = \binom{n+l-1}{l} - \binom{n+l-3}{l-2},$$

$P = P_{l,n}$: ルジャンドル多項式．

(A) $H_l(S^{n-1})$ の正規直交底 $\{\varphi_1, \cdots, \varphi_N\}$ を用いると § 12 の命題 4 より

$$\pi_\eta(\xi) = P_{l,n}(\langle \xi, \eta\rangle) = \frac{a_{n-1}}{N}\sum_{i=1}^{N} \varphi_i(\xi)\varphi_i(\eta)$$

となるから，

---

9) $\varPhi$ の係数体は $\mathbb{R}$ または $\mathbb{C}$.

$$\pi_\eta = \frac{a_{n-1}}{N} \sum_{i=1}^{N} \varphi_i(\eta) \cdot \varphi_i \in \Phi$$

で (A) は O.K.

(B)　§13 の定理 3 (展開定理) にあるように，$\eta_1, \cdots, \eta_N \in S^{n-1}$ を

$$\det(\varphi_i(\eta_j)) \neq 0$$

にとり，

$$E = \{\eta_1, \cdots, \eta_N\}$$

とすれば，

$$\pi_{\eta_j} = \frac{a_{n-1}}{N} \sum_{i=1}^{N} \varphi_i(\eta_j)\varphi_i, \qquad 1 \leqq j \leqq N$$

で $\{\varphi_i\}$ が底だから $\{\pi_{\eta_j}\}$ も底になって (B) も O.K.

こんどは，趣向を変えて奇素数 p により定まる有限体 $\mathbb{F}_p$ を K にとってみよう．さらに K の乗法群 $K^\times$ の指標 $\chi \neq \varepsilon$ を 1 つ定めておく[10)]．また K の加法群 K^+ の指標はちょうど p 個あって，$\alpha \in K$ に対して 1 つずつ定まり，

$$\psi_\alpha(x) = \zeta^{\alpha x}, \qquad \zeta = e^{2\pi i/p}$$

で与えられたことを思い出そう (§3 の (12))．そして，ガウスの和は

$$(1) \qquad \tau_\alpha(\chi) = \sum_{a \in K^\times} \chi(a)\psi_\alpha(a), \qquad \tau(\chi) = \tau_1(\chi)$$

で定義されていた (§3 の (14))．ついでに，

$$(2) \qquad \tau_\alpha(\chi) = \bar{\chi}(\alpha)\tau(\chi) \qquad (\S 5,\ 命題 1)^{11)},$$

$$(3) \qquad \tau(\chi)\tau(\bar{\chi}) = \chi(-1)p \qquad (\S 5,\ 命題 2)$$

も思い出しておこう．そして有限体 $K = \mathbb{F}_p$ 上で次の情況を考える．

$K^n = \mathbb{F}_p{}^n$，　$\langle\ ,\ \rangle$ は K^n の内積，

$S = K^n$，

---

10)　$p = 2$ のときは $K^\times = \mathbb{F}_2{}^\times$ は単位元だけからなるから $\chi \neq \varepsilon$ なる χ はもちろんない．したがって初めから $p \neq 2$ とした．

11)　(2) で $\alpha = 0$ の場合，§7 でやったように $\chi(0) = 0$ と約束すれば

$$\tau_0(\chi) = \sum_{a \neq 0} \chi(a) = 0$$

だから，やはり (2) は O.K.

$$\Phi = \{ f \in L(K^n) \,; f(\alpha x) = \chi(\alpha) f(x),\ x \in K^n,\ \alpha \in K^\times \}.$$

ここに $L(K^n)$ は有限アーベル群 K^n 上の $\mathbb{C}$ に値をとる関数全体の空間である．§3 の定理 1，定理 2 により $L(K^n)$ に内積

$$(4) \qquad \langle f, g \rangle = \frac{1}{p^n} \sum_{x \in K^n} f(x) \bar{g}(x), \qquad f, g \in L(K^n)$$

を定義すれば，K^n の指標

$$(5) \qquad \{\psi_\xi\}_{\xi \in K^n}, \quad \psi_\xi(x) = \zeta^{\langle \xi, x \rangle}, \qquad x \in K^n$$

がヒルベルト空間 $(L(K^n), \langle\ ,\ \rangle)$ の正規直交底になる．

さて，ここが肝心のところであるが，関数

$$P : K \longrightarrow \mathbb{C}$$

を

$$(6) \qquad P(t) \overset{\text{def}}{=} \tau_t(\bar{\chi}) = \sum_{a \in K^\times} \bar{\chi}(a) \psi_t(a)$$

によって定義する．

(A) $\pi_\eta(\xi) = P(\langle \xi, \eta \rangle)$ で定まる π_η が Φ に属すること．すなわち，

$$(7) \qquad \pi_\eta(\alpha \xi) = \chi(\alpha) \pi_\eta(\xi), \qquad \xi, \eta \in S = K^n$$

が成り立つこと．実際，(2) を次のように 2 回用いる：

$$\begin{aligned}
\pi_\eta(\alpha \xi) &= P(\langle \alpha \xi, \eta \rangle) = \tau_{\langle \alpha\xi, \eta \rangle}(\bar{\chi}) \\
&= \chi(\langle \alpha \xi, \eta \rangle) \tau(\bar{\chi}) = \chi(\alpha \langle \xi, \eta \rangle) \tau(\bar{\chi}) \\
&= \chi(\alpha) \chi(\langle \xi, \eta \rangle) \tau(\bar{\chi}) = \chi(\alpha) \tau_{\langle \xi, \eta \rangle}(\bar{\chi}) \\
&= \chi(\alpha) P(\langle \xi, \eta \rangle) = \chi(\alpha) \pi_\eta(\xi), \qquad \text{Q.E.D.}
\end{aligned}$$

(B) $E \subset S = K^n$ を適当に選ぶと $\{\pi_\eta\}_{\eta \in E}$ が Φ の底になること．

K の上の $(n-1)$ 次元の射影空間 $\mathbb{P}^{n-1}(K)$ はよく知られているように集合 $K^n - \{0\}$ に同値関係

$$x \sim y \iff y = \alpha x, \qquad \alpha \in K^\times$$

を入れたときの商空間として定義されている．

$$(8) \qquad \mathbb{P}^{n-1}(K) = (K^n - \{0\}) / K^\times.$$

$K = \mathbb{F}_p$ だから $\mathbb{P}^{n-1}(K)$ は

$$\frac{p^n-1}{p-1}=1+p+p^2+\cdots+p^{n-1}$$

個の元からなる．そこで商空間 (8) の代表元を $\eta_1, \cdots, \eta_N$ として，

(9) $$E=\{\eta_1, \cdots, \eta_N\}, \qquad N=1+p+\cdots+p^{n-1}$$

とおく．我々は $\{\pi_\eta\}, \eta \in E$, が関数空間 Φ の底になることを主張する．これを以下の 3 つの命題に分解して証明する．

命題 1　$\pi_\eta \neq 0, \qquad \eta \in E.$

証明　$\pi_\eta(\xi)=\tau_{\langle\xi,\eta\rangle}(\bar{\chi})=\chi(\langle\xi,\eta\rangle)\tau(\bar{\chi}).$

まず，(3) から $\tau(\bar{\chi}) \neq 0$ である．次に $\eta \neq 0$ だからある ξ があって $\langle\xi,\eta\rangle \neq 0$，したがって $\chi(\langle\xi,\eta\rangle) \neq 0$，すなわち $\pi_\eta(\xi) \neq 0$，Q.E.D.

命題 2　ベクトル空間 Φ は $\{\pi_\eta\}, \eta \in E$, によって張られる．

証明　関数 $f \in L(K^n)$ を任意にとると (5) によって

(10) $$f=\sum_{\xi \in K^n} c_\xi \psi_\xi$$

とフーリエ展開される．この f が Φ に入るための条件を調べて見よう．まず，$\alpha \in K^\times$ に対して，

(11) $$\begin{aligned} f(\alpha x) &= \sum c_\xi \psi_\xi(\alpha x)=\sum c_\xi \zeta^{\langle\xi,\alpha x\rangle}=\sum c_\xi \zeta^{\langle\alpha\xi,x\rangle} \\ &= \sum_\xi c_{\alpha^{-1}\xi}\zeta^{\langle\xi,x\rangle}=\left(\sum c_{\alpha^{-1}\xi}\psi_\xi\right)(x). \end{aligned}$$

したがって，(10), (11) より，

(12) $$\begin{aligned} f \in \Phi \quad &\Longleftrightarrow \quad f(\alpha x)=\chi(\alpha)f(x) \\ &\Longleftrightarrow \quad c_{\alpha^{-1}\xi}=\chi(\alpha)c_\xi, \qquad \xi \in K^n. \end{aligned}$$

とくに $\xi=0$ とおいて，$\chi \neq \varepsilon$ に注意すれば，

(13) $$c_0=0$$

を得る．また，(12) で α^{-1} を α と書き換えれば，

(14) $$f=\sum_{\xi \neq 0} c_\xi \psi_\xi \in \Phi \quad \Longleftrightarrow \quad c_{\alpha\xi}=\bar{\chi}(\alpha)c_\xi, \qquad \alpha \in K^\times$$

となる．したがって，商空間 (8) の代表元の集合 E を用いれば，(14) から，

$$f(x)=\sum_{\xi\neq 0}c_\xi\psi_\xi(x)=\sum_{\eta\in E}\sum_{\alpha\in K^\times}c_{\alpha\eta}\psi_{\alpha\eta}(x)$$

$$=\sum_{\eta\in E}\sum_{\alpha\in K^\times}\bar{\chi}(\alpha)c_\eta\psi_{\alpha\eta}(x)=\sum_{\eta}c_\eta\sum_{\alpha\in K^\times}\bar{\chi}(\alpha)\zeta^{\langle\alpha\eta,x\rangle}$$

$$=\sum_{\eta}c_\eta\sum_{\alpha\in K^\times}\bar{\chi}(\alpha)\zeta^{\langle\eta,x\rangle\alpha}\sum_{\eta}c_\eta\sum_{\alpha\in K^\times}\bar{\chi}(\alpha)\psi_{\langle\eta,x\rangle}(\alpha)$$

$$=\sum_{\eta}c_\eta\tau_{\langle\eta,x\rangle}(\bar{\chi})=\sum_{\eta}c_\eta P(\langle\eta,x\rangle)=\sum_{\eta}c_\eta x_\eta(x).$$

すなわち，

$$f=\sum_{\eta\in E}c_\eta\pi_\eta,\qquad \text{Q.E.D.}$$

命題 3　$\eta,\eta'\in E,\eta\neq\eta'$, ならば
$\langle\pi_\eta,\pi_{\eta'}\rangle=0.$

証明　$$\langle\pi_\eta,\pi_{\eta'}\rangle=\frac{1}{p^n}\sum_{x\in K^n}\pi_\eta(x)\bar{\pi}_{\eta'}(x)=\frac{1}{p^n}\sum_{x}\tau_{\langle\eta,x\rangle}(\bar{\chi})\overline{\tau_{\langle\eta',x\rangle}(\bar{\chi})}$$

$$=\frac{1}{p^n}\sum_{x}\sum_{\alpha\neq 0}\bar{\chi}(\alpha)\zeta^{\langle\eta,x\rangle\alpha}\sum_{\beta\neq 0}\chi(\beta)\zeta^{-\langle\eta',x\rangle\beta}$$

$$=\frac{1}{p^n}\sum_{\alpha,\beta}\bar{\chi}(\alpha)\chi(\beta)\sum_{x\in K^n}\zeta^{\langle\alpha\eta-\beta\eta',x\rangle}=0.$$

なぜなら，η,η' は $\mathbb{P}^{n-1}(K)$ の代表点だから $\alpha\eta-\beta\eta'\neq 0$ となり，$x\longmapsto\xi^{\langle\alpha\eta-\beta\eta',x\rangle}$ はアーベル群 K^n の自明でない指標となり

$$\sum_{x\in K^n}\zeta^{\langle\alpha\eta-\beta\eta',x\rangle}=0$$

となるから，Q.E.D.

命題 1，命題 2，命題 3 から $\{\pi_\eta\},\eta\in E,$ は Φ の直交底となり，(B) の証明が済んだ。

注意　この反省によってルジャンドル多項式とガウスの和がある意味で同じ仕掛けで定義されていることがわかりました。もちろん K や S や Φ のとり方はいろいろありますから，それらに応じて P を拾集すれば面白い変種も見

つかるでしょう．こうなると別々に整数論とか解析とか幾何とかいっていられません．$K=\mathbb{F}_p$（や p-進体）にとれば整数論でしょうし，$K=\mathbb{R}$（や $\mathbb{C}$）にとれば解析でしょうし，図形 S をいろいろと考えれば幾何が入ってまいります．また，ガウスの和やルジャンドル多項式が，より内容のある相互律やラプラス方程式に使用される道具であったように，いろいろの K, S, Φ から得られる変り種の P が役に立つような（相互律やラプラス方程式に類する）面白い応用はないでしょうか？　それとも，いくらガンバッても，ガウスの和やルジャンドル多項式を本質的に凌ぐものはないのでしょうか？

まだ 2 枚ほど原稿用紙が余っています．私は，この連載を書いているときに，ときどきブルフィンチ (Bulfinch, 1796–1867) 作『ギリシア・ローマ神話』（野上弥生子訳，岩波文庫）をめくっておりました．その第 37 章「ピュタゴラス」の部分になかなか面白いことが書いてあると思いました．その一部を引用したいと思います．

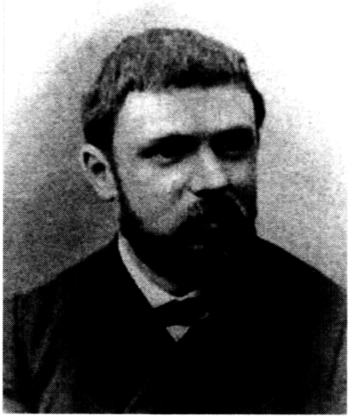
「ピュタゴラスのいうところによると，宇宙のまん中には生命の原力たる中心の火がありました．その中心の火は，地球と，月と，太陽と，及び五つの惑星に圍まれているのでありました．種々の天體間の相互の距離は，音階の比例に符号していると考えられていました．そうして，天體は，その中に住んでいる神々とともに，中心の火を廻って歌いながら合唱舞踊をしている，と想像せられていました．

（中略）　天體は透明なものですから，それを通じてその中にあってともに動いている神々が見られます．これ等の天體は動く時，お互いに摩擦し合うので或る音響を生じて，美妙な階調を作りますが，餘りに幽玄すぎて人間の耳には聞くことができないのでありました．

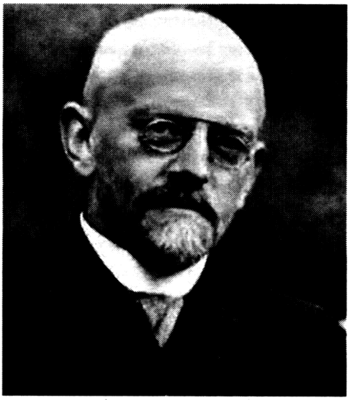
ピュタゴラスはまた堅琴を發明したといわれています」

第2部

ポアンカレの和



ポアンカレ(1854-1912)



ヒルベルト(1862-1943)

第1話
ガウスの和とポアンカレ級数

§1．G-集合

群(group) G が集合(set) X に左から作用するとは，写像 $\varphi: G\times X\to X$ があって，

(1) $\qquad \varphi(1_G, x) = x, \qquad \varphi(st, x) = \varphi(s, \varphi(t, x))$

がすべての $x\in X$ と $s, t\in G$ に対して成り立つことである．1_G は G の単位元．

注意1 多くの場合

$$\varphi(s, x) = sx \qquad \text{または} \qquad {}^{s}x$$

と略記する．すると (1) は

(2) $\qquad 1_G x = {}^{1_G}x = x,$

$\qquad (st)x = s(tx) \qquad$ または $\qquad {}^{st}x = {}^{s}({}^{t}x)$

と簡単になる．${}^{s}x$ の代りに x^s と書いてもよろしいが，(2) の最後の等式はやや不自然な等式

(3) $\qquad x^{st} = (x^t)^s$

になる．特に G が非可換の場合に注意が必要．(注意終)

さて，上のように G が作用している集合 X あるいは対 (G, X) を G-集合

(G-set)とよぶ.

定義 1 G-集合 X に対して記号 $H^0(G, X)$ により X の G の作用による不動点の集合 X^G をあらわす．すなわち

(4) $$H^0(G, X) = X^G = \{ x \in X\,;\, {}^s x = x \ \forall s \in G \}. \qquad \text{(定義終)}$$

注意 2 X が単なる集合であるときはコホモロジー(cohomology)はこれだけである．次第にわかるように，X が群，環，体等々いろいろの構造を持つ場合に高次のコホモロジー

$$H^n(G, X), \qquad n \geqq 0$$

を定義する可能性が出てくる．

§2．G-群

Γ を任意の群とする．さらに Γ は G-集合とすると，§1の (1) により φ: $G \times \Gamma \to \Gamma$ は

$$\varphi(1_G, x) = x, \qquad \varphi(st, x) = \varphi(s, \varphi(t, x))$$

を満足するが，Γ は群だから，その群構造を反映させるために $x, y \in \Gamma$ に対して条件

(1) $$\varphi(s, xy) = \varphi(s, x)\varphi(s, y)$$

を加える．このように G の作用する群のことを G-群(G-group)とよぶ．§1の (2) に対して G-群の場合は

(2) $${}^{1_G}x = x, \qquad {}^{st}x = {}^s({}^t x), \qquad {}^s(xy) = {}^s x \cdot {}^s y$$

が作用の略記である．

G-群 Γ に対してはもちろん不動点集合

$$H^0(G, \Gamma) = \Gamma^G \qquad (\text{§1，定義 1})$$

が定まるが，(2) の追加条件 ${}^s(xy) = {}^s x {}^s y$ から $H^0(G, \Gamma)$ が Γ の部分群になることは明らかである．大切なのは G-群 (G, Γ) に対して **1 次のコホモロジー集合** $H^1(G, \Gamma)$ が定義されることである．まず**コサイクル**(cocycle)(正確に

は1次のコサイクル)を導入する．

写像 $c:G\to\Gamma$ がコサイクルであるとは，条件

(3) $$c(st)=c(s)^{s}c(t),\qquad s,t\in G$$

が成り立っていることと定義する．定義から直ちに

(4) $$c(1_G)=1_\Gamma,\qquad c(s^{-1})={}^{s^{-1}}(c(s)^{-1}).$$

ここに $1_G, 1_\Gamma$ はそれぞれ G,Γ の単位元を表わす．以下 $Z(G,\Gamma)$ でコサイクルの全体を表わす．次に2つのコサイクル c, c' に対して関係 $\sim$ を

(5) $$c'\sim c \iff \begin{cases} \forall s\in G \text{ に対して} \\ \qquad c'(s)=x^{-1}c(s)^{s}x \\ \text{となる } x\in\Gamma \text{ が存在する．}\end{cases}$$

によって定義する．これは $Z(G,\Gamma)$ に同値関係を定義する．そこでこの $\sim$ についての同値類の集合として1次のコホモロジー集合を得る．念のため再記すると，

定義1　G-群 (G,Γ) の1次のコホモロジー集合とは商集合

(6) $$H^1(G,\Gamma)=Z(G,\Gamma)/\sim$$

のことである．ここに $Z(G,\Gamma)$ は (3) を満足する写像(すなわちコサイクル) $c:G\to\Gamma$ の全体で $\sim$ は (5) の同値関係である．

注意1　G-群 (G,Γ) の極めて特別な場合として，

$$^{s}x=x$$

が常に成り立つとき，G の作用は自明(trivial)であるという．このとき $\Gamma^G=\Gamma$ だから

(7) $$H^0(G,\Gamma)=\Gamma.$$

また (3) は

$$c(st)=c(s)c(t),$$

すなわち $c\in \mathrm{Hom}(G,\Gamma)$, $G\to\Gamma$ なる準同型写像の全体，となり，同値関係 (5) も

$$c'(s)=x^{-1}c(s)x$$

と通常の共役関係になってしまう．いま $\mathrm{Int}\,\Gamma$ で群 Γ の内部自己同型写像(inner automorphism)の群を表わせば

(8) $H^1(G, \Gamma) = \mathrm{Hom}(G, \Gamma)/\mathrm{Int}\,\Gamma$

と同一視され，さらに Γ が**可換群**ならば $\mathrm{Int}\,\Gamma = 1$ だから

(9) $H^1(G, \Gamma) = \mathrm{Hom}(G, \Gamma)$

となる．いいかえれば，1次のコサイクルの概念は準同型写像の自然な拡張と考えられる．

§3．G-環

R を単位元 1_R をもつ環(ring)とする．R^+ を R の加法群，$R^\times$ を乗法群とする．R^+ は環の定義により可換群であるが，$R^\times$ は，R が可換環とは仮定しなかったから，一般には非可換である．

G を R に左から作用する群とする．§1, §2 にしたがって $\varphi: G \times R \to R$ を作用を定義する写像とし，$\varphi(s, x) = sx = {}^s x$ の記法を用いると，作用である条件は

(1) $${}^{1_G}x = x, \qquad {}^{st}x = {}^s({}^t x),$$
$${}^s(x+y) = {}^s x + {}^s y, \qquad {}^s(xy) = {}^s x \cdot {}^s y$$

となる．これが成り立っているとき (G, R) を G-環とよぶことは §1, §2 の場合と同様である．

ここで大切なのは，環 R には2つの演算，加法，乗法があり，(1) により G-環 (G, R) は2つの G-群 (G, R^+), $(G, R^\times)$ を自然に従えていることである．われわれの目標は，**$(G, R^\times)$ の1次のコホモロジー類 $\gamma = [c] \in H^1(G, R^\times)$ を用いて (G, R^+) のコホモロジー群 $H^0(G, R^+) = (R^+)^G$ などを捩じる** (twist) **ことの正確な定義を与え，いろいろな数学の実例の構造をわかりやすくする**ことである．詳細は第2話にゆずって，例を主に考えよう．

§4．ガウスの和

G-環 (G, R) が与えられたとき，コサイクル $c \in Z(G, R^\times)$ を1つ選んでおく．定義により(§2の(3))，$c : G \to R^\times$ は条件

(1)　$$c(st) = c(s)^s c(t), \qquad s, t \in G$$

を満足する．そこで $R = R^+$ の部分集合

(2)　$$M_c = M_c(G, R) = \{ x \in R \, ; c(s)^s x = x, \forall s \in G \}$$

を考えると，M_c は R^+ の部分群になる．

例1　$c = 1$, i.e. $c(s) = 1, \forall s \in G$.

この場合は

$$M_c = \{ x \in R \, ; {}^s x = x \} = R^G$$

となって，G による不動点の作る部分環に他ならない．

例2　l を奇素数とし，

$$\zeta = e^{\frac{2\pi i}{l}} \qquad (1 \text{ の原始 } l \text{ 乗根})$$

とする．$K = \mathbb{Q}(\zeta)$ を円の l 分体，$R = \mathcal{O}_K$ を K の整数環，G を $K/\mathbb{Q}$ のガロア群($= \mathrm{Gal}\,(K/\mathbb{Q})$)とする．

$$R = \mathbb{Z}[\zeta] \approx \mathbb{Z}^{l-1}, \qquad \text{また} \qquad G \approx \mathbb{F}_l^\times \quad (\mathbb{F}_l = \mathbb{Z}/l\mathbb{Z}).$$

最後の群同型は $s \in G$ を mod l の整数と同一視できることを意味し，

(3)　$${}^s\zeta = \zeta^s, \qquad s \in G = \mathbb{F}_l^\times$$

が成り立つ(円分体の場合の相互律)[1]．そこで，

$$c(s) = \frac{1-\zeta^s}{1-\zeta}$$

は $Z(G, R^\times)$ のコサイクルである．この c に対して

$$x \in M_c \iff c(s)^s x = x \iff \frac{1-{}^s\zeta}{1-\zeta} {}^s x = x$$

1）　円の l 分体など数論の基本事項については，例えば [O] 参照．

$$\Longleftrightarrow \quad (1-{}^s\zeta)^s x = (1-\zeta)x \quad \Longleftrightarrow \quad (1-\zeta)x \in R^G$$

$$\Longleftrightarrow \quad (1-\zeta)x \in \mathbb{Z} \quad \Longleftrightarrow \quad x \in \left(\frac{1}{1-\zeta}\mathbb{Z}\right) \cap R$$

$$\Longleftrightarrow \quad x \in \frac{l}{1-\zeta}\mathbb{Z}.$$

したがって

$$(4) \qquad M_c = \frac{l}{1-\zeta}\mathbb{Z}, \qquad c(s) = \frac{1-\zeta^s}{1-\zeta}$$

となる．

注意 1　円の l 分体 $K = \mathbb{Q}(\zeta)$ における単数，より正しくは $R = \mathcal{O}_K$ の単数，からなるコサイクル

$$c(s) = \frac{1-\zeta^s}{1-\zeta}$$

はいわゆる円単数(circular units)であって特別のものである[2]．(4) に相等する関係を任意の $\gamma = [c] \in H^1(G, R^\times)$ に対して，さらに同様の結果を一般の円の l^n 分体，$n \geqq 2$，に対して求めることは面白い問題である．そもそも任意の(有限次または無限次の)ガロア拡大 $K/\mathbb{Q}$ について $H^1(\mathrm{Gal}(K/\mathbb{Q}), \mathcal{O}_K{}^\times)$ はどんな構造をもっているか？　知りたいものである．

例 3　これも**例 2** と同様，円の l 分体に関するもので，

$$K = \mathbb{Q}(\zeta), \qquad G = \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{F}_l{}^\times, \qquad R = \mathcal{O}_K = \mathbb{Z}[\zeta]$$

は同じである．違うのはコサイクル

$$c(s) = \left(\frac{s}{l}\right), \qquad \text{ルジャンドル記号(Legendre symbol)}$$

を考えるところである．$c(s)$ の値は $\{\pm 1\}$ だから，ルジャンドル記号が $G = \mathbb{F}_l{}^\times$ の指標であることと $\{\pm 1\} \subset R^\times$ から，c は G-環 R のコサイクルになる[3]．したがって，

2）　[T] 付録 (2) 円分体の類数，参照．

3）　これはちょっと微妙なところで，G の任意の指標 χ をとると，集合 $\{\chi(s), s \in G\}$ は 1 の $(l-1)$ 乗根の集合に属し $R^\times$, $R = \mathcal{O}_K$, には納まらない．

(5) $$M_c = \{ x \in R \,;\, {}^s x = \left(\frac{s}{l}\right) x,\ s \in G \}$$

となる．そこで R の $\mathbb{Z}$ 上の底として $\zeta^t,\ t \in \mathbb{F}_l^{\times}$，をとり，$x \in R$ を

(6) $$x = \sum_t x_t \zeta^t, \qquad x_t \in \mathbb{Z}$$

と書くと

(7) $${}^s x = \sum_t x_t \zeta^{st} = \sum_t x_{s^{-1}t} \zeta^t$$

となるから，特に $x \in M_c,\ c(s) = \left(\frac{s}{l}\right)$ にとると (5), (6), (7) から

$$\sum_t x_t \zeta^t = x = \left(\frac{s}{l}\right) {}^s x = \sum_t \left(\frac{s}{l}\right) x_{s^{-1}t} \zeta^t,$$

すなわち

(8) $$x_t = \left(\frac{s}{l}\right) x_{s^{-1}t}, \qquad \forall s, t \in G.$$

とくに (8) で $s = t$ とおけば，

(9) $$x_t = \left(\frac{t}{l}\right) x_1.$$

これを (6) に代入して

(10) $$x = x_1 \sum_t \left(\frac{t}{l}\right) \zeta^t, \qquad x_1 \in \mathbb{Z}.$$

ここで右辺の和は**ガウスの和**(Gauss sum)である．

(11) $$\tau = \sum_t \left(\frac{t}{l}\right) \zeta^t$$

と書けば，τ が保型性

(12) $${}^s \tau = \left(\frac{s}{l}\right) \tau, \qquad s \in G$$

を持つことは直ちに出るから，(10) より

(13) $$M_c = \mathbb{Z}\tau, \qquad c(s) = \left(\frac{s}{l}\right)$$

がわかった。

例 4 $\mathcal{H}$ を上半平面 $=\{z\in\mathbb{C}\,;\mathrm{Im}\,z>0\}$ とし，$R=\mathcal{O}(\mathcal{H})$ を $\mathcal{H}$ で定義された正則関数(holomorphic functions)の全体とする．これは可換環で $R^\times$ は $\mathcal{H}$ で決して 0 にならない正則関数の全体になる．次に R に作用する群 G として

$$(14)\qquad G=SL_2(\mathbb{Z})=\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix},\ \begin{matrix}a,b,c,d\in\mathbb{Z}\\ ad-bc=1\end{matrix}\right\},$$

すなわちモヂュラー群(modular group)を考える．左作用にするために

$$(15)\qquad s^{-1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix},\qquad s\in G$$

とおく．すると $x=x(\tau)\in R=\mathcal{O}(\mathcal{H})$ に対して G の作用を

$$(16)\qquad {}^s x(\tau)=x(s^{-1}\tau)=x\left(\frac{a\tau+b}{c\tau+d}\right)$$

できめることができる．

$$(17)\qquad c(s)=\frac{1}{(c\tau+d)^4},\qquad s^{-1}=\begin{pmatrix}a & b\\ c & d\end{pmatrix}$$

とおくと $c:G\to R^\times$ がコサイクルになることが確かめられる．実際

$$(18)\qquad c(t)=\frac{1}{(\gamma\tau+\delta)^4},\qquad t^{-1}=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$$

として (16) にしたがって計算すると

$$(19)\qquad {}^s c(t)=\frac{1}{\left(\gamma\dfrac{a\tau+b}{c\tau+d}+\delta\right)^4}.$$

(17), (19) を掛けると

$$(st)^{-1}=\begin{pmatrix}* & *\\ \gamma a+\delta c & \gamma b+\delta d\end{pmatrix}\qquad で$$

$$c(s)^s c(t)=\frac{1}{(\gamma(a\tau+b)+\delta(c\tau+d))^4}$$

$$=\frac{1}{((\gamma a+\delta c)\tau+\gamma b+\delta d)^4}=c(st)$$

となり O.K.

そこで (2) によって加群

$$(20)\qquad M_c=\left\{x\in R\,;\frac{1}{(c\tau+d)^4}x\left(\frac{a\tau+b}{c\tau+d}\right)=x(\tau),\begin{pmatrix}a&b\\c&d\end{pmatrix}\in SL_2(\mathbb{Z})\right\}$$

が考えられる．ここで**例 3** の類似をたどってみよう．そこでは (5) から出発して τ をガウスの和とすれば((11) 参照)

$$M_c=\mathbb{Z}\tau$$

となった((13))．それでは**例 4** の場合 (13) の類似は何であろうか？　ここでは証明しないが，その答は：

$$(21)\qquad M_c=\mathbb{C}G_2,\qquad G_2(\tau)=\sum_{(m,n)\neq(0,0)}\frac{1}{(m\tau+n)^4}$$

となる．ここに，$G_2(\tau)$ はアイゼンシュタイン級数(Eisenstein series)とよばれる級数の最も簡単な場合である[4)]．

注意 2　われわれの本では今後 G-環(G,R)の群 G が有限群の場合に限るので，**例 4** のように無限群 $G=SL_2(\mathbb{Z})$ が出てくる機会はないと思う．しかし有限群の場合(第 2 話)の**ポアンカレの和**(Poincaré sum)の考えは**例 4** に述べたアイゼンシュタイン級数をさらに拡張したポアンカレ級数にヒントを得たものであるから，それを全く説明しないわけにはいかない．

§5．ポアンカレ級数

例 4 のように $G=SL_2(\mathbb{Z})$ を $R=\mathcal{O}(\mathcal{H})$ に作用させる：$x=x(\tau)\in R$ に対して

4）　証明については，例えば [S] p.88 参照．

$$(1)\qquad {}^s x(\tau) = x(s^{-1}\tau) = x\left(\frac{a\tau+b}{c\tau+d}\right), \qquad s^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

整数 $k \geqq 2$ に対して

$$(2)\qquad c(s) = \frac{1}{(c\tau+d)^{2k}}$$

は $G \to R^\times$ のコサイクルになる．**例 4** は $k=2$ の場合であった．アイゼンシュタイン級数 § 4, (21) も

$$(3)\qquad G_k(\tau) = \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^{2k}}$$

に拡張される．$k \geqq 2$ にしておくと (3) は収束して $\mathscr{H}$ 上の正則関数になる．

$M_c = \{\, x \in R\,;\, c(s)^s x = x \,\}$ を考えると

$$(4)\qquad G_k(\tau) \in M_c$$

となっていることも確かめられる．さて，$s^{-1} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ならば $c(s) = 1$ (§ 2 の (4) 参照) で

$${}^s G_k(\tau) = G_k(\tau+1) = G_k(\tau)$$

だから $G_k(\tau)$ は $q = e^{2\pi i\tau}$ の関数になるが，実はテーラー展開，いわゆる q-展開，を持つ：

$$(5)\qquad G_k(\tau) = 2\zeta(2k) + \frac{2(-1)^k(2\pi)^{2k}}{(2k-1)!}\sum_{i=1}^{\infty}\sigma_{2k-1}(i)q^i.$$

ここに

$$\sigma_\nu(i) = \sum_{d|i} d^\nu, \qquad \zeta(s) = \sum_{n=1}^{\infty}\frac{1}{n^s}$$

（リーマン(Riemann)のゼータ関数）.

そこで c が (2) で与えられたとき，

$$(6)\qquad \mathscr{M}_c = \{\, f \in M_c,\ f \text{ は } q\text{-展開をもつ} \,\}$$

なる M_c の部分空間を c-保型形式(c-modular form)の空間とよぶ．すると

$$(7)\qquad \mathscr{M}_c = \mathbb{C}G_k, \qquad k = 2, 3, 4, 5, 7^{5)}$$

5） $k=6$ は跳んでいます．

を証明することができる．これを§4, (13) と比較すると**例3**，**例4**の数論と複素関数論という違う設定において，ガウスの和とアイゼンシュタイン級数がよく似た役割を果たしていることに気付く．

アイゼンシュタイン級数 G_k, $k \geqq 2$, (3), は $G = SL_2(\mathbb{Z})$ の部分群

$$H = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} ; h \in \mathbb{Z} \right\}$$

を考えれば，要するにコサイクル $c(s)$ で s を $H\backslash G$ の代表元 $\bar{s}$ に制限したときの和：

$$(8) \qquad G_k = \sum_{\bar{s} \in H\backslash G} c(\bar{s})\ ^{6)}$$

となる．したがって $x \in R$ で H の元で不変なもの，すなわち $\bar{s}$ の関数と見なせるものをとって，まず形式的に

$$(9) \qquad p_c(x) = \sum_{H\backslash G} c(\bar{s})^{\bar{s}}x$$

を考え，この中で $\mathcal{M}_c$ に入るものをとり出せばより多くの c-保型形式が得られるはずである．これがポアンカレの考えであった．とくに

$$(10) \qquad x(\tau) = q = e^{2\pi i \tau}$$

とすると

$$(11) \qquad p_c(q^\nu) = \sum_{H\backslash G} c(\bar{s}) q^\nu, \qquad \nu \geqq 0$$

となり，$p_c(x)$ の大切な特殊値である．**例3**（円の l 分体）の場合でいえば，

$$R = \mathbb{Z}[\zeta], \qquad \zeta = e^{\frac{2\pi i}{l}}, \qquad G = \mathrm{Gal}(K/\mathbb{Q}) = \mathbb{F}_l^\times,$$

$$c(s) = \left(\frac{s}{l}\right)$$

として，$x \in R$ に対して

$$(12) \qquad p_c(x) = \sum_{s \in G} c(s)^s x$$

を (9) の類似と見れば[7]，いかにもポアンカレの和と称すべきもので，その x

6）G が無限群だから，$H = \{ s \in G ; c(s) = 1 \}$ に注意すれば，和を H/G に制限するのは発散を防止するのに最小限必要な要求である．

$=\zeta^\nu$ における値，$\nu=0,1,\cdots,l-1$,

(13) $$p_c(\zeta^\nu)=\sum_G c(s)\zeta^{\nu s}$$

はガウスの和

$$\tau_\nu=\sum_{s\in\mathbf{F}_l^\times}\left(\frac{s}{l}\right)\zeta^{\nu s}$$

に他ならない.

も1つ，言っておきたいことがある. $x=x(\tau)$ を $\mathcal{M}_c$ からとると q-展開が可能だから

(14) $$x(\tau)=a_0+a_1q+a_2q^2+\cdots\cdots$$

と書けるが，$a_0=0$，つまり $x(\infty i)=0$，のとき x は尖点形式(cusp form)という. このような x の全体 $\mathcal{M}_c{}^0$ は $\mathcal{M}_c$ の部分空間になる. $G_k=p_c(1)$ の場合は (5) において $\zeta(2k)\neq 0$ だから尖点形式ではない，すなわち $G_k\notin\mathcal{M}_c{}^0$ であるが，(11) の $p_c(q^\nu)$, $\nu\geqq 1$ はすべて $\mathcal{M}_c{}^0$ であり，さらに $\mathcal{M}_c{}^0$ は $\mathbb{C}$ 上のベクトル空間として $\{p_c(q^\nu)\}_{\nu\geqq 1}$ で張られる[8].

7） $|G|<\infty$ だから $H=1$ にとった.

8） この証明については，例えば [G] p.39 参照.

第2話
問題の提起

§6．ポアンカレの和

第1話では，G を任意の群として，G の作用する環 R とコサイクル $c: G \to R^\times$ を用いて加群

(1) $$M_c = M_c(R) = \{ x \in R ; c(s)^s x = x, \forall s \in G \}$$

を考え，数論と複素関数論からの例を説明した．第2話以降は G は**有限群**と仮定する．するといろいろな量を G の上で和をとることができる．とくにポアンカレの和

(2) $$p_c(x) = \sum_{s \in G} c(s)^s x, \qquad x \in R$$

は加群 R^+ の自己準同型(endomorphism) p_c を与える．以下 p_c の像を P_c であらわす：

(3) $$P_c = \mathrm{Im}\, p_c = \{ y = p_c(x) ; x \in R \}.$$

命題1　$|G|M_c \subset P_c \subset M_c$　($|G|$ は有限群 G の位数).

証明　$P_c \subset M_c$.

$$y = p_c(x) = \sum_t c(t)^t x$$

を P_c から任意にとると

$$ {}^s y = \sum_t {}^s c(t)^{st} x. $$

よって

$$ c(s)^s y = \sum_t c(s)^s c(t)^{st} x = \sum_t c(st)^{st} x = \sum_t c(t)^t x = y, $$

すなわち $y \in M_c$.

次に $x \in M_c$ を任意にとると，定義から $c(s)^s x = x$．この両辺の s に関する和をとれば $p_c(x) = |G|x$ を得る，すなわち $|G|M_c \subset P_c$ である．(証明終)

注意 1　命題 1 より商加群 M_c/P_c は $|G|$-ねじれ(torsion)加群である．

命題 2　2 つのコサイクル $c, c' \in Z(G, R^\times)$ が $c' \sim c$ (§2, (5))ならば

$$ M_c/P_c \approx M_{c'}/P_{c'} $$

である．

証明　定義から

$$ c'(s) = u^{-1} c(s)^s u $$

なる $u \in R^\times$ が存在する．$x \in M_c$ に対して

$$ c'(s)^s(u^{-1}x) = (u^{-1}c(s)^s u)^s u^{-1s} x = u^{-1} c(s)^s x = u^{-1} x $$

だから，$x \longmapsto u^{-1}x$ は

$$ uM_{c'} = M_c $$

を与える．また $y = p_c(x) \in P_c$ をとると，

$$ u^{-1}y = u^{-1} \sum_s c(s)^s x = \sum_s u^{-1} c(s)^s u^s u^{-1s} x $$

$$ = \sum_s c'(s)^s(u^{-1}x) = p_{c'}(u^{-1}x) $$

だから，$y \longmapsto u^{-1}y$ により

$$ uP_{c'} = P_c $$

を与える．(証明終)

注意 2　命題 2 は M_c/P_c の加群としての構造はコホモロジー類 $\gamma = [c]$ によってきまることを意味する．

注意 3　$c = 1$ のときは

$$M_1 = R^G, \qquad P_1 = \{ \sum_s {}^s x, x \in R \} = \mathfrak{N}_G R,$$

ここで

$$\mathfrak{N}_G x = \sum_s {}^s x \qquad (x \text{ のノルム}).$$

これと**注意 2** を合わせて

$$c \sim 1 \implies M_c/P_c = R^G/\mathfrak{N}_G R = \hat{H}^0(G, R^+)$$

となる．この最後はテイト (Tate) の記法である．一般の G では

$$H^0(G, R^+) = R^{+G}$$

であった (§1, 定義 1)．G を有限群とするとノルムが定義できるので $\hat{H}^0(G, R^+)$ が意味をもつ．

さて，一般のコホモロジー類 $\gamma = [c] \in H^1(G, R^\times)$ にもどり，G-群 (G, R^+) の作用 $(x \longmapsto {}^s x)$ を c を用いて捩る (twist) ことにする．つまり G の R^+ への新しい作用 $(x \longmapsto s \circ x)$ を

(4)　$$s \circ x = c(s)^s x$$

によって定義する．これが

$$(st) \circ x = s \circ (t \circ x)$$

を満足することはすぐわかる．このようにして c によって捩られた G-群 R^+ を

(5)　$$(G, R^+)_c$$

と書こう．すると，

$$M_c = \{ x \in R \,;\, s \circ x = x \}, \qquad P_c = \{ \sum_s s \circ x \}$$

だから

(6)　$$M_c/P_c = \hat{H}^0(G, R^+)_c$$

となる．一方 $c' \sim c$ ならば命題 2 により

$$M_c/P_c \approx M_{c'}/P_{c'}$$

だから，(6) の右辺の

$$\hat{H}^0(G, R^+)_c \approx \hat{H}^0(G, R^+)_{c'}$$

となり，

(7) $\qquad \widehat{H}^0(G, R^+)_\gamma, \qquad \gamma = [c]$

と書いてもさしつかえない[1].

定義 1　集合 X の基数(cardinality)を $|X|$ と書く．$\gamma \in H^1(G, R^\times)$ に対して

$$i_\gamma(G, R) = |\widehat{H}^0(G, R^+)_\gamma|$$

を (G, R) の γ における**指数**(index)とよぶ．

注意 4　一般のテイト群 $\widehat{H}^q(G, R^+)_\gamma$ を用いても

(8) $\qquad i_\gamma{}^q(G, R) = |\widehat{H}^q(G, R^+)_\gamma|, \qquad q \in \mathbb{Z}$

が定義できる．このような量を調べてみるのも面白いであろう．

ここで G-環 (G, R) と G'-環 (G', R') の比較について一般的なことを説明しておく．

$$\begin{array}{ccccc}
\phi s' & & x & & {}^{\phi s'}x \\
\cap & & \cap & & \cap \\
G & \times & R & \longrightarrow & R \\
\uparrow{\scriptstyle\phi} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f} \\
G' & \times & R' & \longrightarrow & R' \\
\cup & & \cup & & \cup \\
s' & & f(x) & & {}^{s'}f(x) = f({}^{\phi s'}x)
\end{array}$$

$\Phi = (\phi, f)$ が射(morphism)：$(G, R) \to (G', R')$ とは

(9) $$\begin{cases} \phi : G' \to G, & \text{群準同型}, \\ f : R \to R', & \text{環準同型}, \\ f({}^{\phi s'}x) = {}^{s'}f(x), & s' \in G', x \in R \end{cases}$$

が成り立っていることである．次に $c : G \to R^\times$ をコサイクルとすると，下の図が可換になるように $c' : G' \to R'^\times$ を定めると，これもまたコサイクルにな

1）$(\widehat{H}^0(G, R^+))_\gamma$ なのか $\widehat{H}^0((G, R^+)_\gamma)$ なのか，ちょっと気持ちが悪いが，1つ γ の代表 c をとれば

$$\widehat{H}^0((G, R^+)_c) = M_c/P_c \approx M_{c'}/P_{c'}$$

なのだから O.K.

ることが確かめられる，すなわち

$$c'(s't') = c'(s')^{s'}c'(t').$$

ただし $f^{\times} = f|_{R^{\times}}$.

$$\begin{array}{ccc} G & \xrightarrow{c} & R^{\times} \\ \phi\uparrow & & \downarrow f^{\times} \\ G' & \xrightarrow{c'} & R'^{\times} \end{array} \qquad c' = f^{\times}c\phi$$

また

$$f(M_c) \subset M_{c'}, \qquad f(P_c) \subset P_{c'}$$

となっているので[2)]，

$$f_c : M_c/P_c \to M_{c'}/P_{c'}$$

が定まる．いいかえれば

(10)　$$\Phi_\gamma : \hat{H}^0(G, R^+)_\gamma \to \hat{H}^0(G', R'^+)_{\gamma'}, \qquad \gamma' = [c']$$

なる加群準同型写像が導かれる．

§7．加群 $P_c(G, R)$ と指数 $i_\gamma(G, R)$

§6，定義 1 で指数

(1)　$$i_\gamma(G, R) = |M_c/P_c|$$

を定義したが，§4 の円の l 分体の例，$R = \mathbb{Z}[\zeta]$, $G = \mathbb{F}_l^{\times}$ と特殊な c に対して M_c を求めた．したがって，P_c を求めることができれば i_γ もわかるわけである．§4 の例の番号にならって，

例 1　$c = 1$. このときは

$$M_c = \{\, x \in R\,;\, {}^s x = x, \forall s \in G \,\} = R^G = \mathbb{Z}[\zeta]^G = \mathbb{Z},$$

また

2）$f(P_c) \subset P_{c'}$ はちょっと難かしい．

$$P_c = \{ \sum_s {}^s x = \mathfrak{N}_G\, x, x \in R \}$$

であるが,

$$x = \sum_t x_t \zeta^t, \qquad x_t \in \mathbb{Z}$$

とおくと ${}^s x = \sum_t x_t \zeta^{st}$. よって

$$\mathfrak{N}_G\, x = \sum_s \sum_t x_t \zeta^{st} = \sum_t x_t \sum_s \zeta^{st} = -\sum_t x_t.^{3)}$$

x_t は任意だから

$$P_c = \mathbb{Z}.$$

したがって§6, 命題2から

(2) $\qquad \gamma = 1$ ならば $i_\gamma(G, R) = 1$

がわかった.

例2 $\qquad c(s) = \dfrac{1-\zeta^s}{1-\zeta}$, 円単数.

このときは§4, (4) により

(3) $\qquad M_c = \dfrac{l}{1-\zeta}\mathbb{Z}$

であった. P_c については

(4) $\qquad p_c(\zeta^s) = \sum_t \dfrac{1-\zeta^t}{1-\zeta}\zeta^{st} = \begin{cases} 0\ , & 1 \leqq s \leqq l-2, \\ \dfrac{-l}{1-\zeta}, & s = l-1. \end{cases}$ [4)]

したがって

(5) $\qquad P_c = \dfrac{l}{1-\zeta}\mathbb{Z}.$

(3), (5) から

(6) $\qquad i_\gamma(G, R) = 1, \qquad \gamma = \left[\dfrac{1-\zeta^s}{1-\zeta}\right]$

---

3) $\sum_s \zeta^{st} = \sum_s \zeta^s = \zeta + \zeta^2 + \cdots + \zeta^{l-1} = -1.$

4) $G = \mathbb{F}_l^\times = \{1, 2, \cdots, l-1\}$ の同一視による.

を得る．

例 3　　$c(s)=\left(\dfrac{s}{l}\right)$，ルジャンドル指標．

この場合は § 4，(13) から

(7)　　$M_c=\mathbb{Z}\tau, \qquad \tau=\sum_t\left(\dfrac{t}{l}\right)\zeta^t$，ガウスの和．

一方，§ 5，(12), (13) によれば

(8)　　$p_c(\zeta^s)=\tau_s=\left(\dfrac{s}{l}\right)\tau$

だから

$$P_c\supset\mathbb{Z}\tau=M_c.$$

逆に $P_c\subset M_c$ は既知(§ 6，命題 1)だから，やはり

(9)　　$i_\gamma(G,R)=1, \qquad \gamma=\left[\left(\dfrac{s}{l}\right)\right].$

注意 1　いままで $i_\gamma(G,R)=1$，すなわちコホモロジー

$$\widehat{H}^0(G,R^+)_\gamma=1$$

となる場合だけを扱ってきた．消滅定理の方向のみを追求するならばそれも意味があるが，γ のとり方によって $i_\gamma(G,R)$ が消えたり点いたりする場合も面白い．さらにいろいろの理由もあるが，次の第 3 話では 2 次体に集中しようと思う．

注意 2　上記 **例 3** で，$c(s)=\left(\dfrac{s}{l}\right)$ のとき

$$M_c=P_c=\mathbb{Z}\tau, \qquad \tau=\sum_t\left(\frac{t}{l}\right)\zeta^t$$

を見たのであるが，実は

(10)　　$\tau=\begin{cases}\sqrt{l}, & l\equiv 1\ (4),\\ i\sqrt{l}, & l\equiv 3\ (4)\end{cases}$

がガウスの有名な結果として知られている．その証明と周辺の話題については本書第 1 部第 3 回参照．

第3話
2次体の場合の実験

§8. $H^1(G, R^\times)$ と M_c/P_c

m を平方因子を含まない整数とし，$K = \mathbb{Q}(\sqrt{m})$ を m の定める2次体とする．G を $K/\mathbb{Q}$ のガロア群とする．それは位数2の群だから

$$G = \langle s \rangle, \qquad s^2 = 1$$

と書ける．$R = \mathcal{O}_K$，K の整数環，とする．したがって $R^\times$ は K の(正しくは R の)単数群である．G の $K, R, R^\times$ の作用は $x = a + b\sqrt{m}$, $a, b \in \mathbb{Q}$, に対し

$${}^s x = a - b\sqrt{m}$$

で与えられる．$R = \mathcal{O}_K = \mathbb{Z} + \mathbb{Z}\omega$:

$$(1) \qquad \omega = \begin{cases} \dfrac{1+\sqrt{m}}{2}, & m \equiv 1 \pmod 4, \\ \sqrt{m}, & m \equiv 2, 3 \pmod 4, \end{cases}$$

$$(2) \qquad {}^s\omega = \begin{cases} 1-\omega, & m \equiv 1 \pmod 4, \\ -\omega, & m \equiv 2, 3 \pmod 4. \end{cases}$$

単数群については

$$(3) \qquad R^{\times} = \begin{cases} \{\pm 1, \pm i\}, & m=-1, i=\sqrt{-1}, \\ \{\pm 1, \pm\omega, \pm\omega^2\}, & m=-3, \omega=\dfrac{1+\sqrt{-3}}{2}, \\ \{\pm 1\}, & m<0, m\neq -1, -3, \\ \{\pm\varepsilon^j ; j\in\mathbb{Z}\}, & m>0. \end{cases}$$

$m>0$ の場合,

$$\varepsilon = u + v\omega, \qquad u, v \in \mathbb{Z}$$

を基本単数，すなわち $R^{\times}$ における >1 で最小のものとする．ε は $u+v\omega \in R^{\times}$ で $u>1$ が最小のものといっても同じことである．

さて，任意のコサイクル $c\in Z(G, R^{\times})$ はその s における値 $c(s)$ で

$$N\cdot c(s) = c(s)\cdot {}^s c(s) = c(1) = 1$$

と同一視されるから

$$(4) \qquad Z(G, R^{\times}) = \{c \in R^{\times} ; Nc = 1\}$$

と考えられ，(3) より

$$(5) \qquad Z(G, R^{\times}) = \begin{cases} R^{\times}, & m<0 \text{ または } m>0 \text{ で } N\varepsilon = 1, \\ \{\pm\varepsilon^{2j}, j\in\mathbb{Z}\}, & m>0 \text{ で } N\varepsilon = -1 \end{cases}$$

となる．

また，$R^{\times}$ は可換だから

$$H^1(G, R^{\times}) = Z(G, R^{\times})/\sim = Z(G, R^{\times})/B(G, R^{\times}),$$

ここで

$$\begin{aligned} B(G, R^{\times}) &= \{c\in Z(G, R^{\times}) ; c\sim 1\} \\ &= \{v/{}^s v ; v\in R^{\times}\} \\ &= \{v^2/Nv ; Nv = \pm 1\} \\ &= \begin{cases} \{v^2 ; v\in R^{\times}\}, & m<0 \text{ または } m>0 \text{ で } N\varepsilon=1, \\ \{\pm v^2 ; v\in R^{\times}, Nv=\pm 1\}, & m>0 \text{ で } N\varepsilon = -1, \end{cases} \end{aligned}$$

あるいは (5) を用いて，

$$(6) \qquad B(G, R^{\times}) = \begin{cases} \{v^2 ; v\in R^{\times}\}, & m<0, \\ \{\varepsilon^{2j} ; j\in\mathbb{Z}\}, & m>0 \text{ で } N\varepsilon = 1, \\ \{(-1)^j\varepsilon^{2j} ; j\in\mathbb{Z}\}, & m>0 \text{ で } N\varepsilon = -1. \end{cases}$$

(3), (5), (6) を用いて，

命題 1　$K=\mathbb{Q}(\sqrt{m})$ を 2 次体，R を K の整数環，$m>0$ のとき ε を基本単数とする．そのとき，

$$H^1(G, R^\times)=\begin{cases}\mathbb{Z}/2\mathbb{Z}, & m<0 \text{ または } m>0, N\varepsilon=-1,\\ \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}, & m>0 \text{ で } N\varepsilon=1.\end{cases}$$

さらにコホモロジー類の代表として

$$(7)\qquad \begin{array}{ll}\{1, i\}, & m=-1,\\ \{\pm 1\}, & m<-1 \text{ または } m>0 \text{ で } N\varepsilon=-1,\\ \{\pm 1, \pm\varepsilon\}, & m>0 \text{ で } N\varepsilon=1\end{array}$$

をとることができる．(命題終)

さて，c を (4) の意味で $R^\times$ の元と見たコサイクルとし，例によって

$$M_c=\{\alpha\in R\,;\, c^s\alpha=\alpha\}$$
$$\cup$$
$$P_c=\{p_c(z)=z+c^sz\,;\, z\in R\}$$

を考える．M_c/P_c は 2-ねじれ群である．

以下，

(8)　$c=u+v\omega,\quad u, v\in\mathbb{Z},$

(9)　$\alpha=a+b\omega,\quad z=x+y\omega,\quad \alpha, z\in R$

とおく．2 次体 $K/\mathbb{Q}$ におけるノルム，トレースを N, T とすると，c がコサイクルであることは

(10)　$1=Nc=u^2+v^2N\omega+uvT\omega$

とあらわされ，

(11)　$t=uT\omega+vN\omega$

とすれば (10) は

(12)　$1-u^2=tv$

となる．(11) を用いて

(13)　$\alpha\in M_c \iff a(1-u)=bt,\quad av=b(u+1),$

および

(14)　$p_c(z)=z+c^sz=(1+u)x+ty+(vx+(1-u)y)\omega$

と書かれる．

関係 (12) により，(13) の $\Longleftrightarrow$ の右辺の 2 つと等式のうち，$v \neq 0$ ならば，第 1 の等式は第 2 の等式から導かれるので不用である．一方 $v=0$ ならば (12) から $u=\pm 1=c$ となり，$\alpha \in M_c$ の条件は α が対合(involution) s に関して対称(symmetric)か反対称(antisymmetric)であることに他ならない．

命題 2　$v=0$ ならば

$$M_c/P_c=\begin{cases} 0, & m\equiv 1 \pmod 4 \text{ のとき}, \\ \mathbb{Z}/2\mathbb{Z}, & m\equiv 2,3 \pmod 4 \text{ のとき}. \end{cases}$$

証明　$v=0$ ならば $c=u$. (12) より $c=\pm 1$.

(i)　$c=1$.

$$M_1=\{\alpha\,;{}^s\alpha=\alpha\}=\mathbb{Z},$$
$$P_1=\{z+{}^sz\,;z\in R\}=T(R).$$

$z=x+y\omega$ より

$$Tz=2x+yT\omega=\begin{cases} 2x+y, & m\equiv 1 \pmod 4, \\ 2x, & m\equiv 2,3 \pmod 4. \end{cases}$$

すなわち

$$P_1=\begin{cases} \mathbb{Z}, & m\equiv 1 \ (\mathrm{nod}\ 4), \\ 2\mathbb{Z}, & m\equiv 2,3 \pmod 4. \end{cases}$$

よって，M_1/P_1 は上記の通り．

(ii)　$c=-1$.

$$M_{-1}=\{\alpha\,;-{}^s\alpha=\alpha\},$$
$$0=\alpha+{}^s\alpha=2a+bT\omega=\begin{cases} 2a+b, & m\equiv 1 \pmod 4, \\ 2a, & m\equiv 2,3 \pmod 4. \end{cases}$$

よって

$$M_{-1}=\begin{cases} \mathbb{Z}(1-2\omega), & m\equiv 1 \pmod 4, \\ \mathbb{Z}\omega, & m\equiv 2,3 \pmod 4. \end{cases}$$

さて，$m\equiv 1 \pmod 4$ のときは $\omega=\dfrac{1+\sqrt{m}}{2}$ より $\sqrt{m}=2\omega-1$. よって

$$M_{-1}=\sqrt{m}\,\mathbb{Z}.$$

次に

$$P_{-1} = \{ z - {}^s z \,;\, z \in R \},$$

$$z - {}^s z = y(\omega - {}^s\omega) = \begin{cases} y\sqrt{m}, & m \equiv 1 \pmod 4, \\ 2y\sqrt{m}, & m \equiv 2, 3 \pmod 4 \end{cases}$$

より

$$P_{-1} = \begin{cases} \sqrt{m}\,\mathbb{Z}, & m = 1 \pmod 4, \\ 2\sqrt{m}\,\mathbb{Z}, & m \equiv 2, 3 \pmod 4. \end{cases}$$

よって，M_{-1}/P_{-1} も同じ型をしている．(証明終)

$m = -1, c = i$ のときは $\omega = i, u = 0, v = 1$ でこれを片付けておけば残りの c は $\pm\varepsilon$ だけで，実 2 次体に集中することができる．

命題 3　$m = -1$ (ガウスの数体)，$c = i$ とすれば

$$M_i/P_i = 0.$$

証明　$\alpha = a + bi$ のとき，

$$\alpha \in M_i \iff i^s\alpha = \alpha \iff i(a - ib) = a + bi$$
$$\iff ai + b = a + bi \iff a = b.$$

よって $M_i = (1+i)\mathbb{Z}$.

次に $z = x + yi$ に対し

$$p_i(z) = z + i^s z = x + iy + i(x - iy) = (x+y)(1+i).$$

すなわち $P_i = (1+i)\mathbb{Z}$. (証明終)

さて，実 2 次体 $K = \mathbb{Q}(\sqrt{m})$ のコサイクル

$$c = u + v\omega, \qquad Nc = 1$$

に対して M_c/P_c の構造を定めよう[1]．$v = 0$ の場合はすんでいる (命題 2) から，$v \neq 0$ とする．(14) の直後に注意したように，(13) で第 1 の等式は不用であるから

(15)　$$M_c \approx \{ (a, b) \in \mathbb{Z}^2 \,;\, av = b(u+1) \}$$

となる．次に $z = x + y\omega$ によって (14) より

1）(7) により $c = \pm\varepsilon, N\varepsilon = 1$ で十分であるが．

$$p_c(z) = A + B\omega,$$

ここに

(16)　　$A = (1+u)x + ty, \qquad B = vx + (1-u)y.$

さらに $P_c \subset M_c$ だから

(17)　　$Av = B(u+1)$

となっている．また (16) の B の形から

(18)　　$d = (v, u-1)$　　(最大公約数)

とおけば $d|B$ である．

逆に d を (18) のようにとれば，$d|B$ なるとき $B = vx + (1-u)y$ となる整数 x, y がとれ，$A = (1+u)x + ty$ とおけば

$$p_c(z) = A + B\omega$$

である．したがって

(19)　　$P_c \approx \{ (A, B) \in \mathbb{Z}^2 ; Av = B(u+1), d|B \},$

ここに $d = (v, u-1)$．いま

(20)　　$e = (v, u+1), \qquad u+1 = Ce, \qquad v = De$

とすれば

(21)　　$M_c = D\mathbb{Z} \supset P_c = D\mathbb{Z} \cap d\mathbb{Z}$

が成り立ち，結局

(22)　　$M_c/P_c \approx \mathbb{Z} \Big/ \dfrac{d}{(D, d)}\mathbb{Z}.$

以上，綜合して，

定理 1　$K = \mathbb{Q}(\sqrt{m})$ のコサイクル $c = u + v\omega$ で $v \neq 0$ とする[2)]．

$$d = (v, u-1), \qquad e = (v, u+1), \qquad u+1 = Ce, \qquad v = De$$

とおけば

$$M_c/P_c \approx \mathbb{Z}/\Delta_c\mathbb{Z},$$

2）　$c = u + v\omega$ は $Nc = 1$ なる K の単数で $c \neq \pm 1$ なものと同じである．

ここで $\Delta_c = \dfrac{d}{(D, d)} = \dfrac{ed}{(v, ed)}$.[3)]

系 1 c がコサイクルならば $-c$ もコサイクルであるが,

$$\Delta_c = \Delta_{-c}.$$

証明 $v = 0$ ならば命題 2 ですんでいるから, $v \neq 0$ とする. 定理 1 の記号を用いて $c = u + v\omega, d = (v, u-1), e = (v, u+1)$ とおくと,

$$\Delta_c = \frac{d}{\left(\dfrac{v}{e}, d\right)} = \frac{de}{(v, de)}.$$

そこで $-c = -u + (-v)\omega$ と書くと, $-c$ について $\{d, e\}$ は $\{e, d\}$ と入れかわるだけで, v は符号を変えるだけだから, $\Delta_c = \Delta_{-c}$ を得る. (証明終)

系 1 により指数 $\Delta_c = [M_c : P_c]$ の決定で残っているのは

$$c = \varepsilon, \qquad \text{基本単数}$$

の場合だけである ((7) 参照). これは長くなるので § を改めて説明する.

§ 9. $\Delta_\varepsilon = [M_\varepsilon : P_\varepsilon]$ の実験結果

記号は § 8 を受け継ぐ. すなわち $m > 0$ を任意の平方因子をふくまない整数, $\varepsilon = u + v\omega$ を実 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の基本単数, そして

$$d = (v, u-1), \qquad e = (v, u+1), \qquad \Delta_\varepsilon = \frac{de}{(v, de)}$$

とおく. ε はコサイクルと同一視されているから $N\varepsilon = 1$ の場合に限ってよい (§ 8, (7) 参照). § 8, 定理 1 により

$$\Delta_\varepsilon = [M_\varepsilon : P_\varepsilon] = i_\gamma(G, R), \qquad \gamma = [\varepsilon]$$

だから, Δ_ε を m の言葉に還元できれば指数の理想的な記述ができるわけであ

3) $\Delta_c > 0$ ときめておく. 諸量の符号は無視してよい.

る．

注意 1　§8, (21) と §6，命題 1 から Δ_ε は 1 または 2 である．問題を考えた当初(2003 年の冬)は全く見当がつかなかったので，§8，定理 1 を $m<1000$, $N_\varepsilon=1$，の場合に用いて，Δ_ε を計算することから始めた[4]．その実験結果をじっと見ているうちに，私は次のことが成り立つに違いないと思った：

（I）　$m\equiv 1 \pmod 4$ ならば $\Delta_\varepsilon=1$.

（II）　$m\equiv 2 \pmod 4$ ならば $\Delta_\varepsilon=2$.

（III）　$m\equiv 3 \pmod 4$ のとき，

$$a_s\equiv 1 \pmod 2 \implies \Delta_\varepsilon=1,$$
$$a_s\equiv 0 \pmod 2 \implies \Delta_\varepsilon=2.$$

ここに a_s は $\sqrt{m}$ の連分数展開の“中心値”：

$$\sqrt{m}=[a_0;\overline{a_1,\cdots,a_{s-1},a_s,a_{s-1},\cdots,a_1,2a_0}].$$ [5]

(III) の場合，Δ_ε の小さい m についての分布は次のようになる．

$$\Delta_\varepsilon=1 \quad : \quad m=3,7,11,15,19,23,31,35,43,47,51,59,67,71,79,83,87,91,103,$$

$$\Delta_\varepsilon=2 \quad : \quad m=39,55,95,111,155,183,203,259,295,299,327,355,371,395.$$

ちょっと見てもわかるように，$\Delta_\varepsilon=2$ になる頻度は $\Delta_\varepsilon=1$ に比べて少ない．

§10．(I), (II) の証明[6]

命題 1　$\Delta_\varepsilon=1 \iff de|v.$

証明　§8，定理 1 で $c=\varepsilon$ とおけば明らか．(証明終)

命題 2　$v\equiv 1 \pmod 2 \implies \Delta_\varepsilon=1.$

4）　この計算は Seok-Min Lee 君による．

5）　連分数については §11 で必要事項をまとめる．

6）　§10, §11 の内容は論文［L&O］に従う．

証明　$d=(v, u-1)$, $e=(v, u+1)$ は v の奇因数である．一方 $(u+1, u-1)|2$．したがって $(d, e)=1$．$de|v$ となるから命題 1 に帰する．（証明終）

v が偶数のとき，$\varepsilon=u+v\omega$ は単数だから u は奇数である．以下 $v'=v/2$, $u'=(u-1)/2$ とおく．

命題 3　$d'=(u', v')$, $e'=(v', u'+1)$ とおくと $d'e'|v'$ であり，

$$\Delta_\varepsilon=1 \iff 2d'e'|v'.$$

証明

$$d=(v, u-1)=(2v', 2u')=2d',$$
$$e=(v, u+1)=(2v', 2u'+2)=2e'.$$

d', e' は v' の互いに素な約数だから $d'e'|v'$．また命題 1 より

$$\Delta_\varepsilon=1 \iff de|v \iff 4d'e'|2v' \iff 2d'e'|v'.$$

（証明終）

注意 1　v が偶数のとき

$$\Delta_\varepsilon=2 \iff 2d'e'\nmid v',$$

なぜなら Δ_ε は 1 または 2 であるから．

命題 4　v を偶数とする（したがって u は奇数）．$\nu\geqq 1$ を $2^\nu\|v$ となる整数とする[7]．このとき，

$$\Delta_\varepsilon=2 \iff u\equiv\pm 1 \pmod{2^\nu}.$$

証明　（i）　$\nu=1$ の場合．$v'=v/2$ は奇数であるから $2d'e'\nmid v'$，すなわち $\Delta_\varepsilon=2$．u は奇数だからもちろん右辺の条件も O.K.

（ii）　$\nu\geqq 2$ の場合．

$$\begin{aligned} & u\equiv\pm 1 \pmod{2^\nu} \\ & \quad\iff u+1\equiv 0 \pmod{2^\nu} \quad \text{または} \quad u-1\equiv 0 \pmod{2^\nu} \\ & \quad\iff u'\equiv 0 \pmod{2^{\nu-1}} \quad \text{または} \quad u'+1\equiv 0 \pmod{2^{\nu-1}}. \end{aligned}$$

さて，命題の $\iff$ の証明：

$(\Longleftarrow)$　$u\equiv\pm 1 \pmod{2^\nu}$ より $u'\equiv 0 \pmod{2^{\nu-1}}$ または $u'+1\equiv 0 \pmod{2^{\nu-1}}$．したがって $2^{\nu-1}|v'$ より

7）　ν は $2^\nu|v$ となる最大の整数．

$$2^{\nu-1}|(v', u')(v', u'+1),$$

よって

$$2^{\nu}|2(v', u')(v', u'+1).$$

一方，$2^{\nu}\nmid v'$ だから

$$2(v', u')(v', u'+1) = 2d'e' \nmid v'.$$

これから注意1より $\Delta_\varepsilon = 2$ が出る．

($\Longrightarrow$)　$u \not\equiv \pm 1 \pmod{2^{\nu}}$ とすれば u' と $u'+1$ のどちらも $\not\equiv 0 \pmod{2^{\nu-1}}$．さて，$(v', u') = d', (v', u'+1) = e'$ は互いに素だから $2^{\nu-1}\nmid d'e'$．一方，$d'e'|v'$ (命題3)かつ $2^{\nu-1}|v'$ だから $2d'e'|v'$．したがってまた命題3から $\Delta_\varepsilon = 1$，すなわち $\Delta_\varepsilon \neq 2$ を得る．(証明終)

命題5　v が偶数で $8\nmid v$ ならば

$$\Delta_\varepsilon = 2.$$

証明　命題4の条件 $u \equiv \pm 1 \pmod{2^{\nu}}$ は $\nu = 1, 2$ ならば任意の奇数 u に対し常に成り立つから $\Delta_\varepsilon = 2$ となる．(証明終)

補題1　$\nu \geqq 3$ に対して

$$a^2 \equiv 1 \pmod{2^{\nu}} \iff a \equiv \pm 1 \pmod{2^{\nu}} \quad \text{または}$$
$$a \equiv \pm(2^{\nu-1}-1) \pmod{2^{\nu}}.$$

証明　($\Longleftarrow$)　$(\pm 1)^2 = 1$ および $(\pm(2^{\nu-1}-1))^2 = 2^{2\nu-2}-2^{\nu}+1 \equiv 1 \pmod{2^{\nu}}$ は $2\nu-2 \geqq \nu, \nu \geqq 3$，より O.K.

($\Longrightarrow$)　逆に，$\nu \geqq 3$ のとき

$$(\mathbb{Z}/2^{\nu}\mathbb{Z})^{\times} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{\nu-2}$$

と位数2と位数 $2^{\nu-2}$ の巡回群の直積になる．だから $(\mathbb{Z}/2^{\nu}\mathbb{Z})^{\times}$ には $a^2 \equiv 1 \pmod{2^{\nu}}$ となる $a \pmod{2^{\nu}}$ の数はちょうど4個である．それが補題の右辺にある4つの元である．(証明終)

補題2　$a, b \in \mathbb{Z}$ が

$$a^2 - mb^2 = 1$$

を満足し，$2^{\nu}\|b$，$\nu \geqq 2$，とすれば

$$a \equiv \pm 1 \pmod{2^{\nu+1}}$$

である．

証明　$\nu \geqq 2, 2^{\nu}\|b \Longrightarrow a^2 - mb^2 = 1$ より $a^2 \equiv 1 \pmod{2^{2\nu}}$．補題1から a

$\equiv \pm 1$ または $\pm(2^{2\nu-1}-1) \equiv \mp 1 \pmod{2^{2\nu}}$．さて，$2\nu-1 \geqq \nu+1$ だから $a \equiv \pm 1 \pmod{2^{\nu+1}}$．（証明終）

命題 6　$\varepsilon = u+v\sqrt{m}, v \equiv 0 \pmod 2$ ならば

$$\Delta_\varepsilon = 2.$$

証明　$8 \nmid v$ ならば $\Delta_\varepsilon = 2$ である（命題 5）．また $2^\nu \| v$，$\nu \geqq 3$，ならば $u \equiv \pm 1 \pmod{2^\nu}$（補題 2）．したがって命題 4 からやはり $\Delta_\varepsilon = 2$ である．（証明終）

定理 1　$m \equiv 2 \pmod 4$ ならば

$$\Delta_\varepsilon = 2.$$

$m \equiv 3 \pmod 4$ ならば

$$\Delta_\varepsilon = 1 \iff v \equiv 1 \pmod 2.$$

証明　$m \equiv 2 \pmod 4$ ならば $1 = u^2-mv^2 \equiv u^2-2v^2 \pmod 4$．このとき $u^2 \equiv 1, v^2 \equiv 0 \pmod 4$ が可能な解だから v 偶数で，命題 6 より $\Delta_\varepsilon = 2$.

$m \equiv 3 \pmod 4$ のとき，($\Longleftarrow$) は命題 2，($\Longrightarrow$) は命題 6 による．（証明終）

注意 2　定理 1 の前半は（II）の証明である．後半は，

$$m \equiv 3 \pmod 4 \text{ のとき}，\Delta_\varepsilon = 1 \iff v \equiv 1 \pmod 2$$

という基準を与える．（III）はこれを連分数に翻訳すればよい（次 § 参照）．ついでながら，次の定理 2 は（I）の証明を与える．

定理 2　$m \equiv 1 \pmod 4$ ならば $\Delta_\varepsilon = 1$ である．

証明　命題 2 より $v \equiv 0 \pmod 2$ と仮定してよい．$b = v/2, a = u+v/2$ とすれば $a, b \in \mathbb{Z}$ で

$$\varepsilon = u+v\omega = a+b\sqrt{m}.$$

$$N\varepsilon = 1 = a^2-mb^2 \equiv a^2-b^2 \pmod 4$$

である．可能な場合は $b^2 \equiv 0, a^2 \equiv 1 \pmod 4$ だけである．したがって a は奇数，b は偶数である．次に

$$a^2-mb^2 \equiv 1 \pmod 8$$

を考える．mod 8 で平方数は 0, 1, 4．a は奇数だから $a^2 \equiv 1 \pmod 8$．一方 $b^2 \equiv 0$ または $4 \pmod 8$ で，$m \equiv 1$ または $\equiv 5 \pmod 8$ である．$a^2-mb^2 \equiv 1 \pmod 8$ を考えると，可能な場合は $b^2 \equiv 0 \pmod 8$ だけになる．したがって b

$\equiv 0 \pmod 4$．よって $8|v$．いま $2^\nu \| v$ とする．したがって $\nu \geqq 3$．$2^{\nu-1} \| b$ だから補題2から $a \equiv \pm 1 \pmod{2^\nu}$．$2^\nu \nmid b$ だから

$$u = a-b \equiv \pm 1 - 2^{\nu-1}h \not\equiv \pm 1 \pmod{2^\nu}, \quad 2 \nmid h.$$

よって命題4より $\Delta_\varepsilon = 1$ を得る．（証明終）

§ 11．(III) の証明

$m \equiv 3 \pmod 4$ のときに

$$\Delta_\varepsilon, \qquad \varepsilon = u + v\sqrt{m}$$

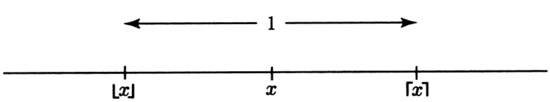
は v の偶奇によって定まる（§ 10，定理1，注意2）．しかし，v の偶奇をもっと直接的に $\sqrt{m}$ の連分数展開によって決めてしまおうというのが本§の問題である[8]．

連分数について必要な基本事項から始めよう．$\alpha = \alpha_0 \in \mathbb{R}$ とする．一般に $x \in \mathbb{R}$ に対して $\lfloor x \rfloor$ によって x を越えない最大の整数をあらわす．通常のガウスの記法では

$$\lfloor x \rfloor = [x]$$

である．ここでは連分数の記法（後出）との衝突を避けるために $\lfloor x \rfloor$ を用いた．$\lfloor x \rfloor$ は x の**床**(flooring) と呼ばれる．ついでながら，これと相対的に x より小さくない最小の整数を $\lceil x \rceil$ と書いて x の**天井**(ceiling) という．要するに $x \in \mathbb{Z}$ ならば

$$x = \lfloor x \rfloor = \lceil x \rceil$$



8）　連分数については［St］がくわしい．

で，$x \notin \mathbb{Z}$ ならば

$$\lfloor x \rfloor < x < \lceil x \rceil, \qquad \lceil x \rceil = \lfloor x \rfloor + 1$$

である．

$\alpha = \alpha_0$ から出発して数列 $\{\alpha_i\}, \{a_i\}$ を

$$a_i = \lfloor \alpha_i \rfloor,$$

$$\alpha_{i+1} = \frac{1}{\alpha_i - a_i}, \qquad \alpha_i \notin \mathbb{Z}$$

という規則で定めて行く[9]．この操作は α_i が $\mathbb{Z}$ に入るまで続ける．もし $\alpha_i \in \mathbb{Z}$ となれば

$$a_i = \lfloor \alpha_i \rfloor = \alpha_i$$

となって続けようがない．このようにして

$$(1) \qquad \alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots \, \cfrac{1}{a_n}}}} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\ddots}}}}$$

となる．(1) を通常

$$(2) \qquad \alpha = [a_0, a_1, \cdots, a_{n-1}, a_n] = [a_0, a_1, a_2, \cdots]$$

と書く[10]．

逆に，任意の整数列 $\{a_n\}_{n \geqq 0}$, $a_n > 0$, $n \geqq 1$，に対して部分連分数 $[a_0, a_1, \cdots, a_n]$ を作ることができ，$[a_0, a_1, \cdots]$ は

$$(3) \qquad \lim_{n \to \infty} [a_0, a_1, \cdots, a_n] = [a_0, a_1, a_2, \cdots]$$

と書ける．

$\alpha \in \mathbb{R}$ に対して

(4) α の連分数展開が有限 $\iff$ $\alpha \in \mathbb{Q}$

は容易にわかるが，さらに

(5) α の連分数展開が周期的 $\iff$ α が 2 次の無理数

9） $\alpha_i = a_i + \dfrac{1}{\alpha_{i+1}}$ となっていることに注意．

10） これは $[a_0, a_1, \cdots, a_{n-1}, a_n]$ が収束するので $\alpha = [a_0, a_1, a_2, \cdots]$ と書くのである．

が成り立つ．ここに (2) の α が**周期的**とは，ある整数 N および正整数 r に対して

$$a_n = a_{n+r}, \qquad \forall n > N,$$

となっていることである．このとき

(6) $$\alpha = [a_0, \cdots, a_N, \overline{a_{N+1}, \cdots, a_{N+r}}]$$

のようにあらわす．このような $r > 0$ の最小のものを 2 次無理数 α の**周期** (period) とよぶ．

(7) 周期 r の 2 次無理数 α が**純周期的**である，すなわち

$\alpha = [\overline{a_0, \cdots, a_{r-1}}]$ となっている

$\Longleftrightarrow$ α は**簡約されている** (reduced)，i.e. $\alpha > 0, -1 < \alpha' < 0$,

ここに α' は α の共役．

(8) α が純周期的であれば，$\alpha = [\overline{a_0, \cdots, a_{r-1}}]$ のとき

$$-\frac{1}{\alpha'} = [\overline{a_{r-1}, \cdots, a_0}]$$

になる．

ここで連分数と 2 次の行列との関係を説明する．

$$\beta \in \mathbb{R}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\beta = \frac{a\beta + b}{c\beta + d}, \qquad a, b, c, d \in \mathbb{Z}, \quad c\beta + d \neq 0$$

と定義する．すると $x \in \mathbb{R}$ に対して

(9) $$[a_0, a_1, \cdots, a_n, x] = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}x$$

が成り立つ．

(10) $$P_n = \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix}\cdots\cdots\begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

とおく．とくに

(11) $$\begin{cases} P_0 = \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}, \\ P_{n+1} = \begin{pmatrix} p_{n+1} & p_n \\ q_{n+1} & q_n \end{pmatrix} = P_n \begin{pmatrix} a_{n+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a_{n+1}p_n + p_{n-1} & p_n \\ a_{n+1}q_n + q_{n-1} & q_n \end{pmatrix}. \end{cases}$$

これから，

$$(12)\qquad \frac{p_n}{q_n}=[a_0, a_1, \cdots, a_n],$$

$$(13)\qquad \det P_n=p_nq_{n-1}-q_np_{n-1}=(-1)^{n+1}$$

を得る．

以下，$\sqrt{m}$ を考える．$a_0=\lfloor\sqrt{m}\rfloor$ とすれば $\alpha=\sqrt{m}+a_0$ は簡約されていることがすぐわかるので，(7) より α は純周期的で，$\lfloor\alpha\rfloor=2a_0$ より $\alpha=[\overline{2a_0, a_1, \cdots, a_{r-1}}]$ とあらわされる．よって

$$\sqrt{m}=\alpha-a_0=[a_0\,;\overline{a_1, \cdots, a_{r-1}, 2a_0}].$$

(8) から

$$-\frac{1}{\alpha'}=-\frac{1}{a_0-\sqrt{m}}=[\overline{a_{r-1}, \cdots, 2a_0}].$$

これから

$$(14)\qquad \sqrt{m}=[a_0\,;\overline{\underbrace{a_1, a_2, \cdots, a_2, a_1, 2a_0}_{r}}]$$

が出る．(対称性)

補題 1　$\sqrt{m}=[a_0\,;\overline{a_1, \cdots, a_{r-1}, 2a_0}]$, $j>0$ に対して

$$\begin{pmatrix} mq_{jr-1} & p_{jr-1} \\ p_{jr-1} & q_{jr-1} \end{pmatrix}=\begin{pmatrix} p_{jr-1} & p_{jr-2} \\ q_{jr-1} & q_{jr-2} \end{pmatrix}\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix}.$$

証明　実際，

$$\sqrt{m}=[a_0, a_1, \cdots, a_{jr-1}, a_0+\sqrt{m}]$$

$$=P_{jr-1}(a_0+\sqrt{m})=\frac{p_{ir-1}(a_0+\sqrt{m})+p_{jr-2}}{q_{jr-1}(a_0+\sqrt{m})+q_{jr-2}}.$$

したがって $1, \sqrt{m}$ の係数を比較して補題の行列の等式を得る．(証明終)

補題 1 の等式の行列式をとって

$$(15)\qquad {p_{jr-1}}^2-m{q_{jr-1}}^2=(-1)^{jr}.$$

いわゆるペル(Pell)方程式

$$x^2-my^2=\pm 1$$

の解は $(\pm p_{jr-1}, \pm q_{jr-1})$ で与えられるものに尽きる．したがって $m\equiv 2,3 \pmod 4$ の場合には基本単数 ε は

(16)　$$\varepsilon = u+v\sqrt{m},\qquad u=p_{r-1},\qquad v=q_{r-1}$$

で与えられる．(15) から

(17)　$$N(\varepsilon)=u^2-mv^2=(-1)^r$$

だから

$$N\varepsilon=1 \iff r\equiv 0 \pmod 2.$$

このことから，(14) の対称性を用いて，

命題 1　$m\equiv 3 \pmod 4$, $N\varepsilon=1$, $\varepsilon=u+v\sqrt{m}$ ならば

$$\sqrt{m}=[a_0\,;\underbrace{\overline{a_1,\,a_2,\,\cdots,\,a_{r/2},\,\cdots,\,a_2,\,a_1,\,2a_0}}_{r}]$$

が $\sqrt{m}$ の展開である．

補題 2　命題 1 の記号を用いて，$s=r/2$ とおくと，

$$v=q_{s-1}(a_sq_{s-1}+2q_{s-2}),$$
$$mv=p_{s-1}(a_sp_{s-1}+2p_{s-2}).$$

証明　まず，

$$P_{r-1}=\begin{pmatrix}a_0&1\\1&0\end{pmatrix}\begin{pmatrix}a_1&1\\1&0\end{pmatrix}\cdots\cdots\begin{pmatrix}a_{s-1}&1\\1&0\end{pmatrix}\begin{pmatrix}a_s&1\\1&0\end{pmatrix}\begin{pmatrix}a_{s-1}&1\\1&0\end{pmatrix}\cdots\cdots\begin{pmatrix}a_1&1\\1&0\end{pmatrix}$$

$$=P_s\left(\begin{pmatrix}a_0&1\\1&0\end{pmatrix}^{-1}P_{s-1}\right)^t=P_sP_{s-1}{}^t\begin{pmatrix}a_0&1\\1&0\end{pmatrix}^{-1}.$$

一方，補題 1 を用いて

(18)　$$\begin{pmatrix}mq_{r-1}&p_{r-1}\\p_{r-1}&q_{r-1}\end{pmatrix}=P_{r-1}\begin{pmatrix}a_0&1\\1&0\end{pmatrix}=P_sP_{s-1}{}^t$$

$$=\begin{pmatrix}p_{s-1}(p_s+p_{s-2})&p_sq_{s-1}+p_{s-1}q_{s-2}\\p_{s-1}q_s+p_{s-2}q_{s-1}&q_{s-1}(q_s+q_{s-2})\end{pmatrix}.$$

ところが，$v=q_{r-1}$ であったから，(18) と (11) の

$$P_{n+1}=P_n\begin{pmatrix}a_{n+1}&1\\1&0\end{pmatrix}$$

から表記の関係を得る．（証明終）

定理 1（(III) の証明）　$m \equiv 3 \pmod 4$, $\varepsilon = u + v\sqrt{m}$, $N\varepsilon = 1$ のとき

$$\sqrt{m} = [a_0\,;\underbrace{\overline{a_1, a_2, \cdots, a_{r/2}, \cdots, a_2, a_1, 2a_0}}_{r}]$$

を周期 r（偶数になる）の連分数展開とすれば，

$$\Delta_\varepsilon = [M_\varepsilon : P_\varepsilon] = 1 \iff a_s,\ s = r/2 \quad (\text{中心値})\text{が奇数},$$

が成り立つ．

証明　補題 2 より

$$v \equiv a_s p_{s-1} \pmod 2, \qquad v \equiv a_s q_{s-1} \pmod 2$$

である．(13) より p_{s-1}, q_{s-1} は互いに素だから，どちらかは必ず奇数である．つまり $v \equiv a_s \pmod 2$．（証明終）

§ 12．いくつかの例

$K/\mathbb{Q}$ を実 2 次体，$K = \mathbb{Q}(\sqrt{m})$, $m > 0$, $m \equiv 3 \pmod 4$ とする．したがって $\omega = \sqrt{m}$ で

$$\mathcal{O}_K = R = \mathbb{Z}[\sqrt{m}], \qquad R^\times = \{\pm 1\} \times \langle \varepsilon \rangle,$$

$$\varepsilon = u + v\sqrt{m} > 0 \text{ が基本単数}$$

である．コサイクル ε による指数 $\Delta_\varepsilon = [M_\varepsilon : P_\varepsilon]$ の決定は，(III) の場合（すなわち $m \equiv 3 \pmod 4$ の場合）が連分数との関連もあり面白いので，理論の復習（そして将来の異なる方法のための予習）を兼ねて 2, 3 の実例を見ておこう．

例 1　$m = 15, \quad \alpha = \sqrt{15},$

$$a_0 = \lfloor \sqrt{15} \rfloor = 3,$$

$$\alpha_1 = \frac{1}{\alpha - a_0} = \frac{1}{\sqrt{15} - 3} = \frac{\sqrt{15} + 3}{6},$$

$$a_1 = \lfloor \alpha_1 \rfloor = 1,$$

$$\alpha_2=\frac{1}{\alpha_1-a_1}=\frac{1}{\frac{\sqrt{15}+3}{6}-1}=\frac{6}{\sqrt{15}-3}$$

$$=\frac{6(\sqrt{15}+3)}{(\sqrt{15}-3)(\sqrt{15}+3)}=\sqrt{15}+3,$$

$$a_2=\lfloor\alpha_2\rfloor=6,$$

$$\alpha_3=\frac{1}{\alpha_2-a_2}=\frac{1}{\sqrt{15}-3}=\alpha_1.$$

すると $a_3=a_1, a_4=a_2, \cdots\cdots$ で

$$\alpha=\sqrt{15}=[3\,;1,6,1,6,\cdots]=[3\,;\overline{1,6}].$$

よって，α の周期 $r=2$, 中心値 $=1=$ 奇数．

§11，(16) より

$$\varepsilon=u+v\sqrt{15},\qquad ここに\quad u=p_{r-1}=p_1, v=q_{r-1}=q_1.$$

また §11，(10), (11) より

$$P_0=\begin{pmatrix}p_0 & p_{-1}\\ q_0 & q_{-1}\end{pmatrix}=\begin{pmatrix}a_0 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix},$$

$$p_0=3,\qquad p_{-1}=1,\qquad q_0=1,\qquad q_{-1}=0.$$

$$\begin{pmatrix}p_1 & p_0\\ q_1 & q_0\end{pmatrix}=P_1=P_0\begin{pmatrix}a_1 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}3 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}4 & 3\\ 1 & 1\end{pmatrix},$$

$$p_1=4,\qquad q_1=1.$$

すなわち $\varepsilon=u+v\sqrt{15}=4+\sqrt{15}$ が基本単数で，

$$N\varepsilon=(4+\sqrt{15})(4-\sqrt{15})=1$$

である．

中心値 $=a_1=1$ (あるいは $v=1$)，奇数，により

$$\Delta_\varepsilon=[M_\varepsilon:P_\varepsilon]=1$$

を得る．

例 2　　$m=39,\qquad \alpha=\sqrt{39},$

$$a_0=\lfloor\sqrt{39}\rfloor=6,$$

$$\alpha_1=\frac{1}{\alpha-a_0}=\frac{1}{\sqrt{39}-6}=\frac{\sqrt{39}+6}{3},$$

$$a_1=\lfloor\alpha_1\rfloor=4,$$

$$\alpha_2 = \frac{1}{\alpha_1 - a_1} = \frac{1}{\frac{\sqrt{39}+6}{3} - 4} = \frac{3}{\sqrt{39}-6} = \frac{3(\sqrt{39}+6)}{3} = \sqrt{39}+6,$$

$$a_2 = \lfloor \alpha_2 \rfloor = 12,$$

$$\alpha_3 = \frac{1}{\alpha_2 - a_2} = \frac{\sqrt{39}+6}{3} = \alpha_1.$$

以下，$a_3 = a_1, a_4 = a_2, \cdots\cdots$ で

$$\alpha = \sqrt{39} = [6\,; 4, 12, 4, 12, \cdots] = [6\,; \overline{4, 12}].$$

α の周期 $r = 2$，中心値 $= 4 =$ 偶数．

$$\varepsilon = u + v\sqrt{39}, \qquad u = p_{r-1} = p_1, \qquad v = q_{r-1} = q_1.$$

$$P_0 = \begin{pmatrix} p_0 & p_{-1} \\ q_0 & q_{-1} \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix},$$

$$p_0 = 6, \qquad p_{-1} = 1, \qquad q_0 = 1, \qquad q_{-1} = 0.$$

$$\begin{pmatrix} p_1 & p_0 \\ q_1 & q_0 \end{pmatrix} = P_1 = P_0\begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 6 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 4 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 25 & 6 \\ 4 & 1 \end{pmatrix},$$

$$p_1 = 25, \qquad q_1 = 4.$$

よって $\varepsilon = u + v\sqrt{39} = 25 + 4\sqrt{39}$ で

$$N\varepsilon = (25 + 4\sqrt{39})(25 - 4\sqrt{39}) = 1.$$

中心値 $= a_1 = 4$ (あるいは $v = 4$)，偶数，により

$$\Delta_\varepsilon = [M_\varepsilon : P_\varepsilon] = 2$$

を得る[11]．

例 3　$m \equiv 3 \pmod 4$, $m < 1000$ のとき，基本単数 $\varepsilon = u + v\sqrt{m}$, $N\varepsilon = 1$, に対する Δ_ε の偶奇(丁半)を書いておこう[12]．

$\Delta_\varepsilon = 1$:

$m =$ 3, 7, 11, 15, 19, 23, 31, 35, 43, 47, 51, 59, 67, 71, 79, 83, 87, 91, 103, 107, 115, 119, 123, 127, 131, 139, 143, 151, 159, 163, 167, 179, 187, 191, 195, 199, 211, 215, 219, 223, 227, 231, 235, 239, 247, 251, 255, 263, 267, 271, 283, 287, 291, 303, 307, 311, 319, 323, 331, 335, 339, 347, 359, 367,

---

11)　本§の例にならって，あなたの好みの m について同様の計算をやってみれば，たちどころに連分数の達人になれます．

12)　これは Seok-Min Lee 君による．

379, 383, 391, 399, 403, 411, 415, 419, 427, 431, 435, 439, 443, 447, 451, 455, 463, 467, 479, 483, 487, 491, 499, 503, 511, 515, 519, 523, 527, 535, 547, 551, 555, 563, 571, 587, 591, 595, 599, 607, 611, 615, 619, 623, 627, 631, 635, 643, 647, 659, 671, 679, 683, 691, 699, 703, 707, 715, 719, 723, 727, 731, 739, 743, 751, 767, 771, 779, 787, 795, 799, 803, 807, 811, 815, 823, 827, 835, 839, 843, 851, 859, 863, 871, 879, 883, 887, 899, 907, 911, 919, 923, 935, 947, 951, 959, 967, 971, 983, 991.

$\Delta_\varepsilon = 2$:

$m =$ 39, 55, 95, 111, 155, 183, 203, 259, 295, 299, 327, 355, 371, 395, 407, 471, 543, 559, 579, 583, 651, 655, 663, 667, 687, 695, 755, 759, 763, 791, 831, 895, 903, 915, 939, 943, 955, 979, 987, 995.

第4話
問題の変形 I
———代数的整数論の復習

§13. ヒルベルト定理 90

問題の設定は第1話，第2話にもどる．すなわち，R を(必ずしも可換でない)環で単位元 $1=1_R$ をもつものとし，G を R に(環自己同型として)作用する**有限群**とする．G は自然に R の乗法群 $R^\times$ に(群自己同型として)作用するから，コホモロジー集合

(1) $$H^1(G, R^\times) = Z(G, R^\times)/\sim$$

が定義される(§2，定義1)．右辺の定義を再記すると

(2) $$Z(G, R^\times) = \{c : G \to R^\times\,;\, c(st) = c(s)^s c(t),\, s, t \in G\}$$

がコサイクル c の集合で，2つのコサイクル c, c' に対し

(3) $$c' \sim c \iff \exists x \in R,\quad c'(s) = x^{-1}c(x)^s x, \qquad s \in G$$

で同値関係が定義されたのであった．

さて，G は有限群と仮定してあるから，第2話で導入したポアンカレの和

(4) $$p_c(x) = \sum_{s \in G} c(s)\, {}^s x, \qquad x \in R$$

を考えることができる．次の定理1は実質的にヒルベルト(D. Hilbert)に負う[1)]．

定理1　R を任意の環，G を R に作用する有限群，$|G| = G$ の位数，とする．$|G|\cdot 1_R \in R^\times$ と仮定する．コサイクル $c \in Z(G, R^\times)$ に対して

$$c \sim 1 \quad (c(s) = x^{-1}\,{}^s x) \iff p_c(\alpha) \in R^\times, \quad \exists \alpha \in R.$$

このとき，

$$c(s) = p_c(\alpha)^s(p_c(\alpha)^{-1})$$

が成り立つ．

証明　($\Longrightarrow$)　$c \sim 1$ とする．$c(s) = \alpha\,{}^s\alpha^{-1}$ なる $\alpha \in R^\times$ がある．(4) で $x = \alpha$ とおくと

$$p_c(\alpha) = \sum_{s \in G} c(s)\,{}^s\alpha = \sum_s \alpha = \alpha|G| \in R^\times.$$

($\Longleftarrow$)　$p_c(\alpha) = \sum_t c(t)\,{}^t\alpha \in R^\times$ とする．両辺に s を作用させ $c(s)$ をかけると，

$$c(s)\,{}^s p_c(\alpha) = \sum_t c(s)\,{}^s c(t)\,{}^{st}\alpha = \sum_t c(st)\,{}^{st}\alpha = \sum_t c(t)\,{}^t\alpha = p_c(\alpha).$$

$p_c(\alpha) \in R^\times$ だから $c \sim 1$ である．同時に

$$c(s) = p_c(\alpha)\,{}^s p_c(\alpha)^{-1}$$

を得る．(証明終)

注意1　定理1の ($\Longleftarrow$) の証明では $|G|\cdot 1_R \in R^\times$，すなわち $|G|$ の位数を R の要素と考えると，R で逆をもつこと，は必要ない．したがって

$$H^1(G, R^\times) = 1$$

を証明するためにはもちろん

$$(5) \qquad \begin{cases} \text{任意のコサイクル } c \text{ に対して} \\ \qquad p_c(\alpha) \in R^\times \\ \text{となる } \alpha \text{ がある} \end{cases}$$

ことを見ればよい．そこで $R = R^\times \cup \{0\}$，すなわち R を(非可換)体(division ring または skew field)とすると，(5) は次の条件にいい直すことができる．

1）このポアンカレとヒルベルトの接点については歴史的な興味がある([R], [Sh] p. 395，参照)．

$$(6)\quad \begin{cases} \text{任意のコサイクル } c \text{ に対して} \\ \qquad p_c(\alpha) = \sum_s c(s)\, {}^s\alpha = 0, \qquad \forall \alpha \in R, \\ \text{ということは起こらない.} \end{cases}$$

さらにここで，R は可換体とし，G を $\mathrm{Aut}\, R$ の有限部分群とすると，$\alpha \longmapsto {}^s\alpha$ が $\alpha, \beta \in R^\times$ に対して ${}^s(\alpha\beta) = {}^s\alpha {}^s\beta$ を満足しているから，いわゆる"指標の1次独立性"の定理[2)]により $c(s) = 0, \forall s \in G$ となり，c がコサイクルなることに矛盾する.

とくにこれを体の有限次ガロア拡大に用いると本来のヒルベルト定理 90 になる[3)].

定理 2 (ヒルベルト定理 90)　K/k を有限次ガロア拡大とすると，

$$H^1(\mathrm{Gal}(K/k), K^\times) = 1.$$

注意 2　§2 でやったように，G-群 Γ が与えられれば第 1 コホモロジー集合 $H^1(G, \Gamma)$ が定義される．いつ

$$H^1(G, \Gamma) = 1$$

となるか(消滅定理，vanishing theorem)がさしあたっての問題である．上記定理 2 は $K^\times$ を $GL_n(K)$ の場合に拡張しても成り立つ[4)]．さらなる拡張についてはクネーザー(M. Kneser)，セール(J.-P. Serre)など参照されるとよい[5)].

§ 14.　$H^1(\mathrm{Gal}(K/k), GL_n(K)) = 1$

§13 のヒルベルト定理 90 は表記のように拡張される.

$G = \mathrm{Gal}(K/k), R = M_n(K), K$ 上の $n \times n$ 行列のつくる環，$R^\times = GL_n(K)$

2）　例えば [L]，p. 283 参照.
3）　ヒルベルト定理 90 は正確には巡回体の場合の定理であった．[H]，Satz 90 参照.
4）　次の § 参照.
5）　[K], [S_2] 参照.

とする．$c: G \to R^\times$ を任意のコサイクルとする．証明したいことは，ある $a \in R^\times$ によって

$$c(s) = a^{-1}\,{}^s a$$

と書けること，あるいは同じことであるが，

$$c(s)\,{}^s b = b, \qquad b \in R^\times$$

と書けることである．

そこで $x \in R$ に対して

$$(1) \qquad p_c(x) = \sum_{t \in G} c(t)\,{}^t x$$

とおく．$p_c(x)$ は $M_n(K)$ の行列であるが，§6，命題1で見たように

$$(2) \qquad c(s)\,{}^s p_c(x) = p_c(x)$$

と書けるので，ある $x \in R$ に対して

$$\det(p_c(x)) \neq 0$$

がいえれば十分である．

そこで k-線型写像 $\pi: K^n \to K^n$ を

$$(3) \qquad \pi(x) = \sum_{s \in G} c(s)\,{}^s x, \qquad x \in K^n$$

と定義する．まず

(4)　　$\mathrm{Im}(\pi)$ は K^n の n 個の独立なベクトルを含む

ことを確かめよう．そのためには，K^n の双対空間 $\mathrm{Hom}_K(K^n, K)$ の元 λ で

$$\lambda(\pi(K^n)) = 0$$

となるものは $\lambda = 0$ に限ることをいえば十分である．さて，$\xi \in K, x \in K^n$ を任意にとれば，λ の仮定により

$$(5) \qquad 0 = \lambda(\pi(\xi x)) = \lambda(\sum_{s \in G} c(s)^s(\xi x)) = \lambda(\sum_s c(s)\,{}^s\xi{}^s x)$$
$$= \lambda(\sum_s {}^s\xi c(s)\,{}^s x) = \sum_s {}^s\xi\lambda(c(s)\,{}^s x).$$

さて，$[K:k] = d$ とし，$\{\xi_1, \cdots, \xi_d\}$ を K の k 上の底とすれば，(5) より

$$(6) \qquad \sum_{s \in G} {}^s\xi_i\lambda(c(s)\,{}^s x) = 0, \qquad 1 \leqq i \leqq d.$$

さて，K/k はガロア拡大だから (6) より $\det({}^s\xi_i) \neq 0$，したがって

$$\lambda(c(s)\,{}^s x) = 0, \qquad x \in K^n, \quad s \in G.$$

とくに $s = 1_G$ とおいて $\lambda(x) = 0$, $\forall x \in K^n$. よって $\lambda = 0$ で (4) が確かめられた．したがって，K^n の底 $v_i, 1 \leqq i \leqq n$, に対して $u_i \in K^n$ を $\pi(u_i) = v_i$ のようにとり，$\{e_i\}$ を K^n の縦ベクトルとしての標準底とし，行列 $a \in M_n(K)$ を $ae_i = v_i$, $1 \leqq i \leqq n$, となるようとれば

$$(7) \qquad p_c(a)e_i = \sum_{t \in G} c(t)\,{}^t a e_i = \sum_t c(t)\,{}^t(ae_i)$$
$$= \sum_t c(t)\,{}^t u_i = \pi(u_i) = v_i, \qquad 1 \leqq i \leqq n$$

を得る．(7) で $\{e_i\}, \{v_i\}$ は底であるから

$$\det p_c(a) \neq 0$$

となり，目的が達せられた．(証明終)

以上まとめてヒルベルト定理 90 の拡張を得る．

定理 1 K/k を有限次ガロア拡大，G をそのガロア群．整数 $n \geqq 1$ に対して $M_n(K)$, n 次の正方行列の環，を自然な G の作用について G-環と見れば，$GL_n(K)$ は G-群で

$$H^1(G, GL_n(K)) = 1$$

である．

§ 15．デデキント整域

K/k が代数体の有限次ガロア拡大，そのガロア群を $G = \mathrm{Gal}(K/k)$ とするとき，G はもちろん K や $K^\times$ に作用するが，さらに K に関連するいろいろな環や群に作用する．その中で最も基本的なものは

$$R = \mathcal{O}_K = K \text{ の整数環}, \qquad R^\times = K \text{ の単数群}$$

である[6)]．ところが，K の場合に簡単であった事柄，たとえばヒルベルト定理

90, i.e. $H^1(G, K^\times) = 1$, に比べて $H^1(G, R^\times)$ を決定することは難しい．実際，$K = \mathbb{Q}(\sqrt{m})$，実2次体，の場合にこの難しさの兆しがあった(第3話，参照)．この方向を進めるのには問題を局所化するのが常道である．K の1つの素点 $\mathfrak{P}$ を選ぶと $\mathfrak{P}$-進体 $K_{\mathfrak{P}}$ ができて，その整数環 $\mathcal{O}_{\mathfrak{P}} = \mathcal{O}_{K_{\mathfrak{P}}}$ はぐっと扱いやすくなる．その代り，大局的，つまり $\mathcal{O}_K$ についてのそもそもの問題と，局所的にばら撒かれた各 $\mathfrak{P}$ における情報をうまくまとめるという手続きが残る．いずれにせよ，$\mathcal{O}_K$ も $\mathcal{O}_{\mathfrak{P}}$ もいわゆるデデキント整域(Dedekind domain)とよばれる可換環の特殊な場合で，代数(algebra)と整数論(arithmetic)の中間に位いし，それを用いて大局と局所をある程度同じ言葉で展開できるのが便利である[7]．

定義1 可換環 A が整域(integral domain)でその任意のイデアル $\mathfrak{a} \neq 0$ が素イデアルの積として書けるとき**デデキント整域**であるという：

(1) $\qquad \mathfrak{a} = \mathfrak{p}_1^{e_1}\mathfrak{p}_2^{e_2}\cdots\mathfrak{p}_g^{e_g}, \qquad \mathfrak{p}_i$ は素イデアル．

注意1 $\mathfrak{a} = A$ を除けば $g \geqq 1, e_i \geqq 1$ で上の表示は一意的である．標語的にいえば，イデアル論の基本定理の成り立つ整域を創始者に敬意を表してデデキント整域とよぶ．

定義2 デデキント整域 A の商体を K とする．K の A-部分加群で有限生成(finitely generated)なものを**分数イデアル**(fractional ideal)という．(定義終り)

分数イデアルの全体 I は A の素イデアルの集合の生成する自由アーベル群をなす．A 自身が I の単位元で，$\mathfrak{a} \in I$ の逆元は

(2) $\qquad \mathfrak{a}^{-1} = \{x \in K\,;\, x\mathfrak{a} \subseteq A\}$

となる．したがって $\mathfrak{a} \in I$ は

(3) $\qquad \mathfrak{a} = \prod_{\mathfrak{p}} \mathfrak{p}^{\nu_{\mathfrak{p}}(\mathfrak{a})}, \qquad \nu_{\mathfrak{p}}(\mathfrak{a}) \in \mathbb{Z}$

---

6) $R^\times = (\mathcal{O}_K)^\times$ のことを K の単数群というのは習慣に従ったまでである．

7) もちろん，$\mathcal{O}_K$ には無数に素イデアルがあるが，$\mathcal{O}_{K_{\mathfrak{P}}}$ には1つしかないのだから，デデキント整域だけで出てくる結果に多くを期待してはいけない．

と一意にあらわされる．通常の A 内のイデアルは (3) の表示で

$$\nu_{\mathfrak{p}}(\mathfrak{a}) \geqq 0$$

がすべての $\mathfrak{p}$ で成り立つものとして定まる．このような整イデアルの全体を I^+ と書く．要するに，$\mathfrak{a} \in I$ に対して

$$\mathfrak{a} \in I^+ \iff \mathfrak{a} \text{ が } A \text{ のイデアル．}$$

例 1　$A = \mathbb{Z}$ はデデキント整域である．$K = \mathbb{Q}$ がその商体．$\mathbb{Z}$ のイデアルはすべて

$$\mathfrak{a} = \mathbb{Z}a, \qquad a > 0$$

と書けるから，$\mathbb{Z}$ がデデキント整域であることは初等整数論の基本定理に他ならない．I は正の有理数全体の作る群と同一視される．$\mathbb{Z}$ には無数の素イデアルがある（ユークリッド『原論』）．

例 2　$A = \mathbb{Z}_p$, p-進整数環（p = 素数）．まず，$a \in \mathbb{Z}, a \neq 0$，に対して

$$\nu_p(a) \geqq 0$$

が (3) のように定まる．$\mathfrak{a} = \mathbb{Z}a$ として $\nu_p(\mathfrak{a})$ をとる．$a \in \mathbb{Q}^\times$ に対しても $\nu_p(a)$ が自然に定義される．例えば

$$\nu_p\left(\frac{1}{p}\right) = -1$$

など．そこで

$$(4) \qquad \begin{cases} |a|_p = p^{-\nu_p(a)}, & a \in \mathbb{Q}^\times, \\ |0|_p = 0 \end{cases}$$

とすると $\mathbb{Q}$ で絶対値 $|\ \ |_p$ が定義される．

$$|ab|_p = |a|_p|b|_p,$$
$$|a+b|_p \leqq \max(|a|_p, |b|_p)$$

が成り立つ．$\mathbb{Q}$ には本来の絶対値 $|a|$ がある．これを $|a|_\infty$ と書く．例えば

$$\left|\frac{1}{p}\right|_\infty = \left|\frac{1}{p}\right| = \frac{1}{p}.$$

一方

$$\left|\frac{1}{p}\right|_p = p \qquad ((4) \text{ 参照}).$$

さて，絶対値があれば距離がある：

$$d(a, b) = |a-b|_\infty.$$

$\mathbb{Q}$ はこの距離について完備(complete)ではない．$\sqrt{2}$ は有理数でいくらでも近似できるが，$\sqrt{2} \notin \mathbb{Q}$．完備でなければ完備化すればよい．このように $\mathbb{Q}$ を $|\ \ |_\infty$ で完備化して $\mathbb{Q}_\infty = \mathbb{R}$，実数体，を得る．$|\ \ |_p$ についても $\mathbb{Q}$ は完備ではない．しかし完備化すれば完備な体 $\mathbb{Q}_p$，p-進体，を得る．

$\mathbb{Z}$ は $\mathbb{Q}$ の部分環だから，$\mathbb{Z}$ の完備化を $|\ \ |_\infty$ について行えば $\mathbb{R}$ の部分環になる．$|\ \ |_\infty$ に関して $\mathbb{Z}$ は $\mathbb{Q}$ で疎(discrete)だから $\mathbb{Z}_\infty = \mathbb{Z} \subset \mathbb{R}$ である．幾何学的イメージは明らかである．しかし $|\ \ |_p$ に関しては $\mathbb{Z}$ は $\mathbb{Q}$ で疎ではない．$|p^n|_p = p^{-n}$ だから，この距離では $\lim_{n\to\infty} p^n = 0$，すなわち 0 は $\{p^n\}$ の集積点である．$\mathbb{Z}$ の $|\ \ |_p$ による完備化 $\mathbb{Z}_p$ は $\mathbb{Q}_p$ の部分環になる．

$\mathbb{Q}$ の絶対値 $|\ \ |_p$ をそのまま自然に $\mathbb{Q}_p$ の絶対値に拡張できる[8]が，$\mathbb{Z}_p$ は

(5)　$$\mathbb{Z}_p = \{a \in \mathbb{Q}_p\,;\, |a|_p \leqq 1\}$$

と特徴づけられる．つまり環 $\mathbb{Z}_p$ は $|\ \ |_p$-円板になる．さらに $\mathbb{Z}_p$ のイデアルはこの円板を縮小してすべて得られる．$n \geqq 1$ に対して

(6)　$$p^n\mathbb{Z}_p = \{a \in \mathbb{Q}_p\,;\, |a|_p \leqq p^{-n}\}$$

がすべての $\mathbb{Z}_p$ のイデアルをつくし，素イデアルは $p\mathbb{Z}_p$ 1 つしかない．もちろん $\mathbb{Z}_p$ はデデキント整域である．そして $\mathbb{Q}_p$ はその商体である．

(7)　$$\mathbb{Z}_p/p\mathbb{Z}_p \approx \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p, \qquad p\text{ 元体},$$

が成り立つ．

さて，$\mathbb{Q}$ から $|\ \ |_\infty$，$|\ \ |_p$ による完備化によって $\mathbb{R}, \mathbb{Q}_p$ なる 2 種類の完備体を得たが，片や連結，片や完全非連結といった違いも著しいが，数論の観点からすると，$\mathbb{R}$ がいま一歩で代数閉体 $\mathbb{C}$ に達する $(\mathbb{R}(i) = \mathbb{C})$ というのに 1 の冪(べき)根は $\{\pm 1\}$ と 2 つしかないのに反し，$\mathbb{Q}_p$ は((7) にヘンゼル(Hensel)の補題を用いて証明されるように) 1 の $(p-1)$ 乗根を含むという事実である．

8）$\mathbb{Q}_p \in \alpha = \lim_{n\to\infty} a_n$, $a_n \in \mathbb{Q}$ のとき $|\alpha|_p = \lim_{n\to\infty} |a_n|_p$.

§ 16. デデキント整域の拡大

A をデデキント整域，K を A の商体，L を K の n 次の拡大体とする．$x \in L$ が **A の上で整である** (integral over A) とは，x が多項式環 $A[X]$ のモニック (monic) 多項式[9]の零点 (あるいは根) になっていることと定義する．A 上の整元全体を B とする．すると，

命題 1 上記の記号のもとに B もデデキント整域で L はその商体である (この B を A の L における**整閉包** (integral closure) とよぶ)．

$\mathfrak{p}$ を A の素イデアルとする．集合 $\mathfrak{p}B = \{\sum_i \alpha_i\beta_i\,;\,\alpha_i \in \mathfrak{p}, \beta_i \in B\}$ は B のイデアルになるが，多くの場合 $\mathfrak{p}B = \mathfrak{p}$ と略記する．これは上手に情況を判断する限り極めて便利な記法なので使うことにしよう．ただしこのように B に拡張されたイデアル $\mathfrak{p}$ は最早素イデアルとは限らない．

(1) $$\mathfrak{p} = \mathfrak{P}_1^{e_1}\mathfrak{P}_2^{e_2}\cdots\mathfrak{P}_g^{e_g}$$

のごとく分解する．さて，$\mathfrak{P}_i$ は B の素イデアルであるから $B/\mathfrak{P}_i$ は体である．$A/\mathfrak{p}$ は自然に $B/\mathfrak{P}_i$ の部分体となる．この拡大の次数を

$$f_i = f_i(\mathfrak{P}_i|\mathfrak{p})$$

と書く．

(2) $$f_i = [B/\mathfrak{P}_i : A/\mathfrak{p}]$$

命題 2 上記 (1), (2) の記号のもとに，L/K が**分離的** (separable) であれば[10]

$$\sum_{i=1}^{g} e_i f_i = n = [L:K].$$

注意 1 A, K, L, B は上の通りとし，$\mathfrak{P}$ を B の素イデアル，$\mathfrak{p} = \mathfrak{P} \cap A$ (こ

9) 最高次の係数 = 1 なる多項式をモニックとよぶ．

10) 将来われわれは標数 $\mathrm{ch}(K) = 0$ の場合のみを考えるから，命題 2 の等式は常に O.K.

れは A の素イデアル)とする．このとき $\mathfrak{P}$ は (1) の分解の素因子 $\mathfrak{P}_i$ の1つとしてあらわれる．$\mathfrak{P}^\lambda \| \mathfrak{p}$ で $\mathfrak{P}^\lambda$ が $\mathfrak{p}$ を割ること，すなわち $\mathfrak{P}^\lambda \supset \mathfrak{p}$ を意味するとすれば，(1) の e はこのような λ の最大数であるから $\mathfrak{P}^e \| \mathfrak{p}$ と書く．この $e \geqq 2$ のとき $\mathfrak{P}$ は L/K で**分岐**する(ramified)という．また $e=1$ かつ $B/\mathfrak{P}$ が $A/\mathfrak{p}$ の分離拡大のとき $\mathfrak{P}$ は L/K で**不分岐**(unramified)という[11]．

例1　$\mathbb{Z}$ はデデキント整域でその商体は有理数体 $\mathbb{Q}$．k を代数体，すなわち $\mathbb{Q}$ の有限次拡大とすると $\mathbb{Z}$ の k における整閉包 $\mathcal{O}_k$ はデデキント整域で，k の整数環とよばれる．さらに K を k の有限次拡大とすると，$K/\mathbb{Q}$ も有限次拡大だから，$\mathbb{Z}$ の K における整閉包すなわち K の整数環 $\mathcal{O}_K$ が定まるが，$\mathcal{O}_K$ は同時に $\mathcal{O}_k$ の K における整閉包になっている．$\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアルとすれば $\mathcal{O}_k/\mathfrak{p}$ は有限体で，$p=\mathfrak{p}\cap\mathbb{Z}$ なる素数を用いて $\mathcal{O}_k/\mathfrak{p} \approx \mathbb{F}_{p^f}$，ここに $f=[\mathcal{O}_k/\mathfrak{p}:\mathbb{Z}/p\mathbb{Z}]$ である．

例2　例1の $\mathbb{Z}$ を§15，例2の p-進整数環 $\mathbb{Z}_p$ におき代えるとその商体 $\mathbb{Q}_p$，p-進体，の有限次拡大 k，すなわち局所体，の中に $\mathbb{Z}_p$ の整閉包 $\mathcal{O}_k$ が定まる．この場合には p は k においてただ1つの素因子 $\mathfrak{p}$ をもつだけである．しかも $\mathfrak{p}$ は単項イデアル $\mathfrak{p}=(\pi)=\pi\mathcal{O}_k$ である．π は素元(prime element)で，単数群 $\mathcal{O}_k^\times$ を除いて一意的に定まる[12]．e, f に関しては

$$p=\mathfrak{p}^e, \qquad [\mathcal{O}_k/\mathfrak{p}:\mathbb{Z}_p/p\mathbb{Z}_p] = f$$

と簡単にきまる．

例3　K/k を代数体の有限次拡大，$\mathfrak{P}$ を K の，すなわち $\mathcal{O}_K$ の素イデアル，$\mathfrak{p}$ を $\mathfrak{p}=\mathfrak{P}\cap\mathcal{O}_k$ で定まる $\mathcal{O}_k$ の素イデアルとする．

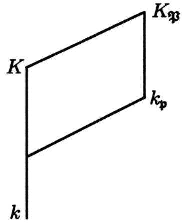
$\mathfrak{P}$ の K/k に関する分岐指数 e は $\mathfrak{P}^e \| \mathfrak{p}$ で定義された．デデキント整域 $\mathcal{O}_k$，$\mathcal{O}_K$ における $\mathfrak{p}, \mathfrak{P}$ に関する位数を与える関数を $\nu_\mathfrak{p}, \nu_\mathfrak{P}$ とする[13]．$\mathfrak{p}=\mathfrak{P}^e$ だから，$\mathfrak{p}$ を K で考えれば

$$\nu_\mathfrak{p}(\mathfrak{p})=1, \qquad \nu_\mathfrak{P}(\mathfrak{p})=e$$

11)　将来われわれが考えるのは $\mathrm{ch}(K)=0$ および $A/\mathfrak{p}$ が有限体の場合なので，分離性は自働的に成り立っている．

12)　$k^\times$ の元は $\alpha=u\cdot\pi^r, u\in\mathcal{O}_k^\times, r\in\mathbb{Z}$，と一意的にあらわせる．$\mathbb{C}^\times \ni \alpha = re^{i\theta}$ (極座標)と似ている．

13)　$\mathfrak{a}\in I$ に対して $\mathfrak{a}=\prod_\mathfrak{p} \mathfrak{p}^{\nu_\mathfrak{p}(\mathfrak{a})}$ できまる関数 $\mathfrak{a}\longmapsto\nu_\mathfrak{p}(\mathfrak{a})\in\mathbb{Z}$ のこと．$a\in K^\times$ に対しては $\nu_\mathfrak{p}(a)=\nu_\mathfrak{p}((a))$ で与える，$(a)=a\mathcal{O}_k\in I$.



である．$k_{\mathfrak{p}}$ は k の絶対値 $|\ \ |_{\mathfrak{p}}$,

$$|a|_{\mathfrak{p}} = N\mathfrak{p}^{-\nu_{\mathfrak{p}}((a))}, \qquad a \in k^{\times}$$

による完備化である．同様に $K_{\mathfrak{P}}$ は K の $\mathfrak{P}$ についての完備化で，$k_{\mathfrak{p}}$ は $K_{\mathfrak{P}}$ 内での k の閉包と同一視される．

いま $K = k(\alpha)$ とし，$f(X) \in k[X]$ を α の k 上の最小多項式とする．$f(X) \in k_{\mathfrak{p}}[X]$ と考えて

$$\text{(3)} \qquad f(X) = f_1(X)f_2(X)\cdots f_g(X)$$

を $k_{\mathfrak{p}}[X]$ での既約分解とし，$f_i(\alpha_i) = 0, \alpha_i \in \bar{k}$，を $f_i(X)$ の根とする．ただし $f_1(\alpha) = 0$ としておく．

$$K = k(\alpha) \approx k(\alpha_i) = K_i$$

の k 上の同型があるから，K の素イデアル $\mathfrak{P}$ に K_i の素イデアル $\mathfrak{P}_i$ が対応し，

$$k_{\mathfrak{p}}(\alpha_i) = K_{\mathfrak{P}_i}, \qquad 1 \leqq i \leqq g$$

が成り立つ．さらに

$$\text{(4)} \qquad k_{\mathfrak{p}} \otimes_k K \approx \bigoplus_{i=1}^{g} K_{\mathfrak{P}_i}$$

が導かれる．

トレース，ノルムについて

$$\text{(5)} \qquad \begin{cases} T_{K/k}(x) = \sum_{\mathfrak{P}|\mathfrak{p}} T_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(x), \\ N_{K/k}(x) = \prod_{\mathfrak{P}|\mathfrak{p}} N_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}(x), \qquad x \in K. \end{cases}$$

が成り立つ．

§ 17．ガロア拡大

A をデデキント整域，K を A の商体，L/K を有限次ガロア拡大，B を L 内の A の整閉包，そして $G = \mathrm{Gal}(L/K)$ とする．まず，

命題 1　$\mathfrak{p}$ を A の素イデアル，$\mathfrak{P}_1, \cdots, \mathfrak{P}_g$ を $\mathfrak{p}$ の B における相異なる拡張からなる素イデアルとすると，群 G は集合 $\{\mathfrak{P}_1, \cdots, \mathfrak{P}_g\}$ の推移的置換群(transitive permutation group)である．

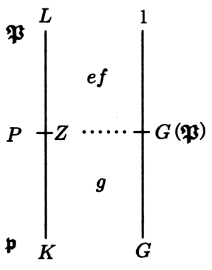
命題 2　命題 1 の記号を用いて，A の素イデアル $\mathfrak{p}$ の B における素因子分解(§ 16, (1), (2) 参照)において，$e_1 = \cdots = e_g, f_1 = \cdots = f_g$ である．この共通の値を e, f とすると

$$n = [L : K] = efg$$

となる．

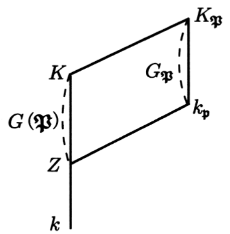
命題 3　ガロア拡大 $L/K, G$ は命題 1 の通りとする．L の素イデアル $\mathfrak{P}$ の固定群 $G(\mathfrak{P}) = \{s \in G\,; {}^s\mathfrak{P} = \mathfrak{P}\}$ の位数 $= ef, [G : G(\mathfrak{P})] = g$．$G(\mathfrak{P})$ を $\mathfrak{P}$ の L/K における分解群(deomposition group)という．$G(\mathfrak{P})$ に対応する L/K の中間体を Z，$P = \mathfrak{P} \cap Z$ とおくと

$$e(\mathfrak{P}|P) = e(\mathfrak{P}|\mathfrak{p}),$$
$$f(\mathfrak{P}|P) = f(\mathfrak{P}|\mathfrak{p}),$$
$$e(P|\mathfrak{p}) = f(P/\mathfrak{p}) = 1$$



である．Z を $\mathfrak{P}$ の L/K に関する**分解体**という．

例 1　§16，例 3 の情況で K/k が代数体のガロア拡大，$G=\mathrm{Gal}(K/k)$ とする．$\mathfrak{P}$ を K の素イデアル，$\mathfrak{p}=\mathfrak{P}\cap k$ を k の素イデアルとする．$\mathfrak{P}$ による K の局所化を $K_{\mathfrak{P}}$ とすると $k_{\mathfrak{p}}$ は $K_{\mathfrak{P}}$ の部分体であったが，$K=k(\alpha)$，$f(X)\in k[X]$ を α の最小多項式とすれば $K_{\mathfrak{P}}=k_{\mathfrak{p}}(\alpha)$ であったから，α の $k_{\mathfrak{p}}$ 上の最小多項式 $g(X)\in k_{\mathfrak{p}}[X]$ は $f(X)$ を割る．K/k はガロア拡大と仮定してあるから $f(X)$ は K で分裂(split)し，したがって $g(X)$ は $K_{\mathfrak{P}}$ で分裂する．よって $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ もガロア拡大である．$G_{\mathfrak{P}}=\mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$ とおく．



さて，$s\in G=\mathrm{Gal}(K/k)$ をとると

$$|{}^s a|_{{}^s\mathfrak{P}}=|a|_{\mathfrak{P}},\qquad a\in K$$

となっているので，$s\in G(\mathfrak{P})$, i.e. ${}^s\mathfrak{P}=\mathfrak{P}$，ならば，$s$ は距離を不変にする．よって s は連続であり，そもそも k を不変にするから $k_{\mathfrak{p}}$ の各元も不変にする．したがって $G(\mathfrak{P})\to G_{\mathfrak{P}}$ の準同型 φ が定まるが，明らかに φ は単射である．さらに $|G(\mathfrak{P})|=ef=|G_{\mathfrak{P}}|$ だから全単射．換言すれば $K\cap k_{\mathfrak{p}}=Z$, $\mathfrak{P}$ の分解体，が出た．

§18．問題の再記

われわれは第 2 話で G を有限群と仮定して G-環 R を考え，G-群 $R^{\times}$ のコサイクル $\gamma=[c]\in H^1(G,R^{\times})$ によって捩じったテイト・コホモロジー群 $\hat{H}^0(G,R^{+})_{\gamma}$ を研究することを提案した．

さて，現実的には 1 つのコサイクル $c: G \to R^\times$ に対して

$$M_c = \{x \in R\,;\, c(s)\,{}^s x = x,\ \forall s \in G\}$$

（重さ c の保型元の加群）

とその部分加群

$$P_c = \{p_c(x) = \sum_{s \in G} c(s)\,{}^s x,\ x \in R\}$$

（ポアンカレの和のつくる加群）

を考え，商 M_c/P_c を研究することであった．この指数 $[M_c : P_c]$ を $i_\gamma(G, R)$ と書いた（§ 6, § 7）．

第 3 話は，2 次体 $K/\mathbf{Q}$ のガロア群 G, $|G| = 2$，が K の整数環 R に作用するという極めて特別な場合の実験報告であった．

この第 4 話では，ここまで復習した代数的整数論の枠内で，第 3 話の実験のできる限りの拡張を試みようと思う．題して‘問題の変形(Ｉ)’という．§ 14 で述べたヒルベルト定理 90

$$H^1(\mathrm{Gal}(K/k), GL_n(K)) = 1$$

がこの問題の変形にいかに大切であるかを示そう．

§ 19．問題の変形(Ｉ)

A をデデキント整域，K を A の商体とする．以下 K の**標数** $\mathrm{ch}(K) = 0$ と仮定する．L を K の有限次ガロア拡大，B を L における A の整閉包，$G = \mathrm{Gal}(L/K)$，ガロア群とする．$R = M_n(B)$ を環 B 上の n 次の正方行列環，$n \geqq 1$ とする．したがって群 $R^\times = GL_n(B)$ となる．この G-環 R について $\widehat{H}^0(G, R^+)_\gamma$ あるいは M_c/P_c, $\gamma = [c] \in H^1(G, R^\times)$ を研究したい．

さて，§ 14，定理 1 のヒルベルト定理 90（の拡張）は

(1)　　$H^1(G, GL_n(L)) = 1$

となる．コサイクル $c: G \to R^\times = GL_n(B)$ は $B \subset L$ より $G \to GL_n(L)$ のコ

サイクルと考えられる．したがって (1) により

(2) $c(s) = \xi^{-1}\,{}^{s}\xi, \quad \xi \in GL_n(L)$

なる ξ が存在する．この ξ は必ずしも $GL_n(B)$ に入るわけではない．では，どのような行列か？

まず，L の元は A の元をかけることで分母を払うことができるので

(3) $\xi \in GL_n(L) \cap M_n(B)$

と仮定してよろしい．いま η を ξ と同様に (3) を満足するコサイクル (2) の解とする．すると，$\xi^{-1}\,{}^{s}\xi = \eta^{-1}\,{}^{s}\eta$ だから $a \in GL_n(K)$ によって $\eta = a\cdot\xi$ となる．

$x \in R = M_n(B), s \in G = \mathrm{Gal}(L/K)$ に対して

$$x \in M_c \iff c(s)^{s}x = x \iff \xi^{-1}\,{}^{s}\xi^{s}x = x$$
$$\iff {}^{s}(\xi x) = \xi x \iff \xi x \in M_n(A).$$

したがって

(4) $$M_c = \{x \in M_n(B)\,;\, \xi x \in M_n(A)\}$$
$$= M_n(B) \cap \xi^{-1}M_n(A)$$

あるいは

(5) $\xi M_c = (\xi M_n(B))^{G}.$

いま環 $R = M_n(B)$ 内の右イデアル ξR を単に (ξ) と略記することにすれば，(5) は

(6) $\xi M_c = (\xi)^{G}$

となる．

次にポアンカレの和の方であるが，

$$y = p_c(x) = \sum_t c(t)^{t}x = \sum_t \xi^{-1}\,{}^{t}\xi^{t}x$$
$$= \xi^{-1}\sum_t {}^{t}(\xi x) = \xi^{-1}T_{L/K}(\xi x).$$ [14)]

したがって (6) の記法によって

(7) $\xi P_c = T_{L/K}((\xi))$ [15)]

---

14) $\alpha \in M_n(L)$ に対して $T_{L/K}\,\alpha = \sum_{t\in G} {}^{t}\alpha$ と書いた．

15) $(\xi) = \xi\cdot R$

と書ける．(6), (7) から，$\gamma=[c]\in H^1(G,R^\times)$として，

(8)　　$\hat{H}^0(G,R^+)_\gamma=M_c/P_c=(\xi)^G/T_{L/K}((\xi))$

と見やすくなる．また ξ を $a\eta,\ a\in GL_n(K)$ でおきかえても (8) の最右辺は変わらないことに注意しておく．

注意 1　ヒルベルト定理 90 が $R=M_n(B)$ に使えたので，無造作に $(\xi)=\xi R$ と書いてスイスイと (8) など書いてしまった．しかし R のように行列環内の整環の右イデアル論は，局所体に限っても，あまり楽なものではない[16]．(8) に現れる (ξ) の正体はまだわからない．これを問題追求の一段落と見てこの第 4 話の題を‘問題の変形（I）’とした所似である．

$n=1$ とすると $R=B$ で通常の代数的整数論である．B は可換だからイデアルの左右に気を使わないですむ．この場合には十分に詳しい分岐理論(ramification theory)が使える．問題の変形(II)が具体的に見えてくる．第 3 話の 2 次体の実験で，他の体では了解に苦しむ‘$\sqrt{m}$ の連分数展開の中心値の丁半’の正しい解釈も期待できるのである．

16)　[D], [A] 参照．

第5話
問題の変形 II
———分岐理論

§ 20．共役差積と判別式

A をデデキント整域，K をその商体，その**標数** $\mathrm{ch}(K)=0$, L を K の有限次拡大体，B を A の L における整閉包とする．さらに A の任意のイデアル $\mathfrak{a}\,(\neq 0)$ に対して**商環** $A/\mathfrak{a}$ **は有限環である**と仮定する[1)]．以下，これらの附帯条件はいちいちことわらないことにする．

体 L の分数イデアル $\mathfrak{A}\in I_L$ (§ 15，定義 2 参照)に対して

(1) $$\mathfrak{A}^*=\{x\in L\,;\,T_{L/K}(x\mathfrak{A})\subset A\}$$

とおく．

命題 1 (i) $\mathfrak{A}^*$ はまた L の分数イデアルである．

(ii) $\mathfrak{A}\in I_L{}^+$ (すなわち $\mathfrak{A}\subset B$)ならば

$$(\mathfrak{A}^*)^{-1}\in I_L{}^+.$$ [2)]

定義 1 $\mathfrak{D}_{L/K}=(B^*)^{-1}$ (これは命題 1(ii)により B のイデアル)を L/K の

1） k を有限次代数体，$\mathcal{O}_k$ をその整数環，$\mathfrak{p}$ を $\mathcal{O}_k$ の素イデアル，$k_\mathfrak{p}$を k の $\mathfrak{p}$ における完備化，$\mathcal{O}_{k_\mathfrak{p}}$ を $k_\mathfrak{p}$ の整数環とする．$A=\mathcal{O}_k$ または $\mathcal{O}_{k_\mathfrak{p}}$ のとき上の仮定はすべて O.K.である．

2） § 15，(2) 参照．

共役差積(different)という．

命題2　$M/L/K$ を体の塔で，M における B(したがって A)の整閉包を C とすれば，すべてのイデアルを C 内で考えて

$$\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L}\mathfrak{D}_{L/K}.$$

定義2　$D_{L/K} = N_{L/K}\mathfrak{D}_{L/K}$ を L/K の判別式(discriminant)という．

命題3　体の塔 $M/L/K$ に対して

$$D_{M/K} = (N_{L/K}D_{M/L})D_{L/K}{}^{[M:L]}.$$

定理1(デデキントの判別定理)　L/K を拡大体，$\mathfrak{P}$ を L の素イデアル，$\mathfrak{p} = \mathfrak{P} \cap K$, e を $\mathfrak{P}$ の L/K に関する分岐指数，i.e. $\mathfrak{P}^e \| \mathfrak{p}$ とする．このとき

(i)　$\mathfrak{P} \nmid e \iff \mathfrak{P}^{e-1} \| \mathfrak{D}_{L/K}$. [3)]

(ii)　$\mathfrak{P} \mid e \iff \mathfrak{P}^{e} \mid \mathfrak{D}_{L/K}$. [4)]

定理2　K/k を代数体の有限次拡大とする．

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{P}^{t_{\mathfrak{P}}}$$

を K/k の共役差積の素因子分解とすると，局所体の拡大 $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ について

$$\mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} = \mathfrak{P}^{t_{\mathfrak{p}}}$$

となる．ここで右辺の $\mathfrak{P}$ は $\mathcal{O}_{K_{\mathfrak{P}}}$ の素イデアルと見る．この意味で

$$\mathfrak{D}_{K/k} = \prod_{\mathfrak{P}} \mathfrak{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$$

が成り立つ．

注意1　この定理は，共役差積の決定には局所拡大 $K_{\mathfrak{P}/k_{\mathfrak{p}}}$ だけを考えればよいことを意味する．

ここで，また一般の拡大体 L/K の場合にもどって大切な命題を1つやっておこう．

命題4　$\mathfrak{a} \in I_K, \mathfrak{B} \in I_L$ をそれぞれイデアルとする．このとき

---

3)　この場合，分岐は**従順**(tame)であるという．とくに $e=1 \Longleftrightarrow \mathfrak{P} \nmid \mathfrak{D}_{L/K}$ は(i)の場合だから，不分岐ならば従順になる．したがって分岐する $\mathfrak{P}$ は有限個である．

4)　この場合，分岐は**野性的**(wild)であるという．

$$\mathfrak{a} \mid T_{L/K}\mathfrak{B} \iff \mathfrak{a} \mid \mathfrak{B}\mathcal{D}_{L/K}$$

が成り立つ．

証明 左辺の $T_{L/K}\mathfrak{B}$ が K のイデアルであることはすぐわかる．次に，

$$\begin{aligned} \mathfrak{a} \mid T_{L/K}\mathfrak{B} &\iff \mathfrak{a} \supset T_{L/K}\mathfrak{B} \\ &\iff \mathcal{O}_K \supset \mathfrak{a}^{-1}T_{L/K}\mathfrak{B} \\ &\iff \mathcal{O}_K \supset T_{L/K}(\mathfrak{a}^{-1}\mathfrak{B}) \\ &\iff \mathfrak{a}^{-1}\mathfrak{B} \subset \mathcal{O}_L{}^* = \mathcal{D}_{L/K}{}^{-1} \\ &\iff \mathfrak{B}\mathcal{D}_{L/K} \subset \mathfrak{a} \\ &\iff \mathfrak{a} \mid \mathfrak{B}\mathcal{D}_{L/K}. \qquad \text{(証明終)} \end{aligned}$$

系 1 $\mathfrak{a} \in I_K$ のとき

$$\mathfrak{a} \mid T_{L/K}\mathcal{O}_L \iff \mathfrak{a} \mid \mathcal{D}_{L/K}.$$

§ 21. 不動イデアル

L/K をガロア拡大，$G = \mathrm{Gal}(L/K)$, A をその商体が K となるデデキント整域，そして B を L における A の整閉包とする．G は I_L, L のイデアル群，に作用する：$\mathfrak{A} \longmapsto {}^s\mathfrak{A}$, $\mathfrak{A} \in I_L$ と書く．ヒルベルトにならって

$${}^s\mathfrak{A} = \mathfrak{A}, \qquad \forall s \in G,$$

となる $\mathfrak{A}$ を**不動イデアル**(ambiguous ideal)とよぼう[5]．

$\mathfrak{A} = \mathfrak{a}B, \mathfrak{a} \in I_K$ の場合に ${}^s\mathfrak{A} = \mathfrak{A}$ は明らかであるから $\mathfrak{A}$ は不動である．

逆は成り立たない．実際 2 次体 $K = \mathbb{Q}(\sqrt{m})$ の単項イデアル $\mathfrak{A} = (\sqrt{m})$ は ${}^s\!\sqrt{m} = -\sqrt{m}$ だから不動であるが，$\mathfrak{A} = a\mathcal{O}_K$ なる $a \in \mathbb{Q}$ はない．すなわち $\mathfrak{A}$ は $\mathbb{Q}$ のイデアルの延長にはなれない．

一般の場合にもどって，L の素イデアル $\mathfrak{P}$ は $\mathfrak{p} = \mathfrak{P} \cap K$ によって K の素イデアルを定める．しかしこの $\mathfrak{p}$ から見れば L の素イデアル $\mathfrak{P}'$ で $\mathfrak{p} = \mathfrak{P}' \cap$

5） [H]，§ 57 参照．

K となるものは $\mathfrak{P}$ 以外にもあり得る．実際§17，命題1，命題2により $\mathfrak{P}'$ は $\mathfrak{P}$ のある共役 ${}^s\mathfrak{P}$ であり，分岐指数 $e_{\mathfrak{P}} = e_{{}^s\mathfrak{P}}$ が成り立つ．この共通の値を $e_{\mathfrak{p}}$ と書くことにすれば

$$(1)\qquad \mathfrak{p} = \Big(\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}\Big)^{e_{\mathfrak{p}}}$$

と書くことができる．ここで $\mathfrak{P}|\mathfrak{p}$ は $\mathfrak{p}$ の L におけるすべての相異なる素因子を動く．以下，簡単のために

$$(2)\qquad \mathfrak{p}^{\#} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$$

という記法を用いると

$$(3)\qquad \mathfrak{p} = \mathfrak{p}^{\# e_{\mathfrak{p}}}.$$

ここで左辺は $\mathfrak{p}$ を L で考えたものである．

さて，$\mathfrak{A} \in I_L{}^+$ を任意にとると

$$(4)\qquad \mathfrak{A} = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{m_{\mathfrak{P}}}, \qquad m_{\mathfrak{P}} \geqq 0$$

という形に L で素因子分解できる．したがって (4) より，

$$(5)\qquad {}^s\mathfrak{A} = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}} {}^s\mathfrak{P}^{m_{\mathfrak{P}}} = \prod_{\mathfrak{p}}\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{m_{s^{-1}\mathfrak{P}}}.$$

さらに素因子分解の一意性から (4), (5) より

$$(6)\qquad {}^s\mathfrak{A} = \mathfrak{A} \iff \mathfrak{A} = \prod_{\mathfrak{P}} \mathfrak{P}^{m_{\mathfrak{P}}} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$$

ここに $m_{\mathfrak{p}} = m_{\mathfrak{P}},\ \mathfrak{P}\,|\,\mathfrak{p}.$

次に，不動イデアル $\mathfrak{A}$ を (6) のように $m_{\mathfrak{p}}$ を用いてあらわし，$\mathfrak{a} = \mathfrak{A} \cap K$ の素因子分解を求めてみよう．まず

$$(7)\qquad m_{\mathfrak{p}} = q_{\mathfrak{p}}e_{\mathfrak{p}} + r_{\mathfrak{p}}, \qquad 0 \leqq r_{\mathfrak{p}} \leqq e_{\mathfrak{p}} - 1$$

と書くと，§11で定義した記号を用いて (7) より

$$(8)\qquad q_{\mathfrak{p}} = \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} - \frac{r_{\mathfrak{p}}}{e_{\mathfrak{p}}} = \left\lfloor \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor.$$

さて，$\mathfrak{p}^{\# m_{\mathfrak{p}}} = \mathfrak{p}^{\# q_{\mathfrak{p}} e_{\mathfrak{p}}}\mathfrak{p}^{\# r_{\mathfrak{p}}} = \mathfrak{p}^{q_{\mathfrak{p}}}\mathfrak{p}^{\# r_{\mathfrak{p}}}$．よって

$$(9)\qquad \begin{cases} \mathfrak{p}^{\#m_\mathfrak{p}} \cap K = \mathfrak{p}^{q_\mathfrak{p}}(\mathfrak{p}^{\#r_\mathfrak{p}} \cap A) \\ \qquad\qquad\quad = \mathfrak{p}^{\left\lfloor \frac{m_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor}(\mathfrak{p}^{\#r_\mathfrak{p}} \cap A). \end{cases}$$

次に

$$(10)\qquad \mathfrak{p}^{\#r_\mathfrak{p}} \cap A = \begin{cases} A, & r_\mathfrak{p} = 0, \\ \mathfrak{p}, & r_\mathfrak{p} > 0. \end{cases}$$

実際 $x \in K$ に対して,

$$\mathfrak{p}^{\#r_\mathfrak{p}} = \mathfrak{P}_1{}^{r_\mathfrak{p}}\mathfrak{P}_2{}^{r_\mathfrak{p}}\cdots\mathfrak{P}_g{}^{r_\mathfrak{p}}, \qquad \mathfrak{P}_1 = \mathfrak{P}$$

と書くと,

$$\begin{aligned} x \in \mathfrak{p}^{\#r_\mathfrak{p}} \quad &\Longleftrightarrow \quad \nu_\mathfrak{P}(x) \geqq r_\mathfrak{p} \\ &\Longleftrightarrow \quad \nu_\mathfrak{p}(x) \geqq \frac{r_\mathfrak{p}}{e_\mathfrak{p}} \\ &\Longleftrightarrow \quad \nu_\mathfrak{p}(x) \geqq \begin{cases} 0, & r_\mathfrak{p} = 0 \\ 1, & r_\mathfrak{p} > 0 \end{cases} \\ &\Longleftrightarrow \quad x \in \begin{cases} A, & r_\mathfrak{p} = 0 \\ \mathfrak{p}, & r_\mathfrak{p} > 0. \end{cases} \end{aligned}$$

これを (9) にもどして

$$(11)\qquad \mathfrak{p}^{\#m_\mathfrak{p}} \cap K = \mathfrak{p}^{\left\lceil \frac{m_\mathfrak{p}}{e_\mathfrak{p}} \right\rceil}$$

と書ける.

以上まとめると,

命題 1 ガロア拡大 L/K に対して不動イデアル

$$\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\#m_\mathfrak{p}} \in I_L{}^+, \qquad \mathfrak{p}^\# = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}$$

を考えれば,

$$\mathfrak{A} \cap K = \prod_{\mathfrak{p}} \mathfrak{p}^{\left\lceil \frac{m_\mathfrak{p}}{e_\mathfrak{p}} \right\rceil}$$

が成り立つ.

次に，$\mathfrak{A} \in I_L{}^+$ を不動イデアルとし，$T_{L/K}\mathfrak{A}$ の K における素因子分解を求めよう．まず § 20，命題 4 により

(12)　$$\mathfrak{p}^\lambda \mid T_{L/K}\mathfrak{A} \iff \mathfrak{p}^\lambda \mid \mathfrak{A}\mathscr{D}_{L/K}.$$

補題 1　$\mathscr{D}_{L/K}$ は不動イデアルである．

証明　$\mathscr{D}_{L/K} = (B^*)^{-1}$ (§ 20，定義 1) だから，B^* が不動なことをいえばよい．§ 20，(1) により $B^* = \{x \in L\,;\, T_{L/K}(xB) \subset A\}$．$x \in B^*$ をとると，$T_{L/K}({}^s xB) = T_{L/K}(xB) \subset A$．ゆえに ${}^s x \in B^*$．すなわち ${}^s B^* \subset B^*$．s^{-1} について同様に論じて ${}^s B^* = B^*$．(証明終)

さて，(12) の情況にもどり，不動イデアル $\mathfrak{A}$, $\mathscr{D}_{L/K}$ に (6) の表示を用いて

(13)　$$\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_\mathfrak{p}}$$
$$\mathscr{D}_{L/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_\mathfrak{p}}$$

とおけば，(12) の右辺について

(14)　$$\begin{aligned} \mathfrak{p}^\lambda \mid \mathfrak{A}\mathscr{D}_{L/K} &\iff \mathfrak{p}^{\# e_\mathfrak{p}\lambda} \mid (\mathfrak{p}^\#)^{m_\mathfrak{p}+t_\mathfrak{p}} \\ &\iff e_\mathfrak{p}\lambda \leqq m_\mathfrak{p}+t_\mathfrak{p} \\ &\iff \lambda \leqq \left\lfloor \frac{m_\mathfrak{p}+t_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor . \end{aligned}$$

したがって (12), (14) より，

命題 2　L/K の不動イデアル $\mathfrak{A} \in I_L{}^+, \mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_\mathfrak{p}}$，に対して

$$T_{L/K}\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left\lfloor \frac{m_\mathfrak{p}+t_\mathfrak{p}}{e_\mathfrak{p}} \right\rfloor} .$$

§ 22. 問題の変形(II)

第4話§19問題の変形(I)で，$n=1$ の場合を再記する．A をデデキント整域，K をその商体，L を K の有限次ガロア拡大，B を A の L における整閉包，そして§20の冒頭で述べたように $\mathrm{ch}(K)=0, A/\mathfrak{A}$ は有限環，$\mathfrak{A}\in I_K{}^{+}$，を仮定する．もちろん $G=\mathrm{Gal}(L/K)$，ガロア群．そこで§19の (1),…, (8) を $n=1$ として要約すると次のようになる．

(1) $\qquad H^1(G, L^\times)=1$

よりコサイクル $c: G\to B^\times$ に対して

(2) $\qquad c(s)=\xi^{-1}\,{}^s\xi, \qquad \xi\in L^\times$

なる ξ がとれる．さらに

(3) $\qquad \xi\in B, \qquad \xi\neq 0$

と仮定できる．次に

(4) $\qquad M_c=\{x\in B\,;\xi x\in A\}=B\cap\xi^{-1}A$

あるいは

(5) $\qquad \xi M_c=(\xi B)^G.$

B 内のイデアル ξB を (ξ) と略記すれば，(5) は

(6) $\qquad \xi M_c=(\xi)^G$

となる．

次に，ポアンカレの和については，

$$p_c(x)=\xi^{-1}T_{L/K}(\xi x), \qquad x\in B$$

となるから，

(7) $\qquad \xi P_c=T_{L/K}((\xi))$

(6), (7) から，$\gamma=[c]\in H^1(G, B^\times)$ として，

(8) $\qquad \widehat{H}^0(G, B^+)_\gamma=M_c/P_c=(\xi)^G/T_{L/K}((\xi))$

となる．

補題1 (2), (3) における ξ の生成するイデアル (ξ) は不動イデアルであ

る．

証明　(2) より ${}^s\xi = c(s)\xi$, $\forall s \in G$. $c(s) \in B^\times$ だから，上の両辺のイデアルをとって $({}^s\xi) = {}^s(\xi) = (\xi)$，すなわち (ξ) は不動である．(証明終)

§21 命題1，命題2 を $\mathfrak{A} = (\xi)$ として (8) に適用すると，次の大切な定理を得る．

定理1　K をデデキント整域 A の商体，L を K のガロア拡大，B を A の L における整閉包，K の標数 $= 0$，$A/\mathfrak{a}$ は有限，$\mathfrak{a} \in I_K{}^+$，とする．$\gamma = [c]$ を $H^1(G, B^\times)$ のコサイクル類，$\xi \in B$ を $c(s) = \xi^{-1}\,{}^s\xi$ を満たす元，

$$(\xi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$$

を不動イデアル(補題1)の素因子分解，また L/K の共役差積 $\mathcal{D}_{L/K}$ の素因子分解を

$$\mathcal{D}_{L/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}},$$

$e_{\mathfrak{p}}$ を L/K における素イデアル $\mathfrak{p}$ の分岐指数 $(= e(\mathfrak{P}|\mathfrak{p}))$ とする．さらに

$$M_c = \{x \in B\,;\, c(s)^s x = x, \forall s \in G\} \supset$$

$$P_c = \{p_c(x) = \sum_{s \in G} c(s)^s x, x \in B\}$$

をコサイクル c に属する B 内の保型元の加群とポアンカレの和の生成する部分加群とすると，加群同型：

$$\widehat{H}^0(G, B^+)_\gamma = M_c/P_c \approx \prod_{\mathfrak{p}} \mathfrak{p}^{\left\lfloor \frac{m_{\mathfrak{p}} + t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil}$$

が成り立つ．

これから直ちに次の指数定理を得る．

定理2　記号は定理1と同じ．

$$i_\gamma(G, B) = |\widehat{H}^0(G, B^+)_\gamma| = [M_c : P_c]$$

$$= \prod_{\mathfrak{p}} (N\mathfrak{p})^{\left\lfloor \frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil},$$

ここで $N\mathfrak{p} = |A/\mathfrak{p}|$.

注意 1　上の定理 1, 定理 2 において, $\hat{H}^0(G, B^+)_\gamma$ を決める不変量は $e_{\mathfrak{p}}, t_{\mathfrak{p}}, m_{\mathfrak{p}}$ であるが, $e_{\mathfrak{p}}, t_{\mathfrak{p}}$ はガロア拡大 L/K に固有のもので, 実際に大切なのは $m_{\mathfrak{p}}$ である. この $m_{\mathfrak{p}}$ はコサイクル c の解 $c(s) = \xi^{-1}\,{}^s\xi$ ((2) 参照)の生成する不動単項イデアル (ξ) の素因子分解 $(\xi) = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$ によって定まる. したがって定理 1 だけでは $\hat{H}^0(G, B^+)_\gamma$ を決定するという問題の真の解決とはいい難い. 実際, 定理 1 は標数 $= 0$ と $A/\mathfrak{p}$ の有限性の仮定のもとに一般のデデキント整域に対して成り立つ. したがって任意の代数体のガロア拡大 K/k とその局所体のガロア拡大 $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ に対して同時に成り立っている. だから, 以下に述べるように定理 1 により問題が局所体の場合に帰着されたと理解したい. 同時にこれはわれわれを局所体の場合のより徹底した研究に駆り立てる.

§ 23. 諸定理

§ 20 の冒頭の仮定のもとに, § 20 定理 1 (i) より L/K で分岐する $\mathfrak{P}$ は共役差積 $\mathfrak{D}_{L/K}$ の素因子である有限個のみであり, さらに L/K がガロア拡大であれば

$$e(\mathfrak{P} \mid \mathfrak{p}) = e_{\mathfrak{p}}, \qquad \forall \mathfrak{P} \mid \mathfrak{p}$$

であり, $t_{\mathfrak{p}}$ も不動イデアル $\mathfrak{D}_{L/K}$ によって

$$\mathfrak{D}_{L/K} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}}$$

として定まる. したがって § 20 定理 1, (i), (ii) は基礎体 K の言葉で

$$(1) \qquad \begin{cases} \mathfrak{p} \nmid e \iff e_{\mathfrak{p}} - 1 = t_{\mathfrak{p}} \\ \mathfrak{p} \mid e \iff e_{\mathfrak{p}} \leqq t_{\mathfrak{p}} \end{cases}$$

といい直すことができる.

補題1 有限個の$\mathfrak{p}$を除いて

$$\left\lfloor \frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil = 0.$$

実際，有限この$\mathfrak{p}$を除いて$e_{\mathfrak{p}}=1, t_{\mathfrak{p}}=0$だから，上の差はどんな$m_{\mathfrak{p}}$をとっても$m_{\mathfrak{p}}-m_{\mathfrak{p}}=0$.

注意1 L/Kが不分岐ガロア拡大ならば常に$e_{\mathfrak{p}}=1, t_{\mathfrak{p}}=0$だから，どんな$m_{\mathfrak{p}}$をとっても上の補題にあらわれる差$=0$. したがってどんな$\gamma=[c] \in H^1(G, B^{\times})$をとっても$\hat{H}^0(G, B^+)_{\gamma}=0$である．実は，

定理1 L/Kが従順なガロア拡大ならば

$$\hat{H}_0(G, B^+)_{\gamma}=0, \qquad \forall \gamma \in H^1(G, B^{\times}).$$

証明 §22 定理1の記号を継いで

$$\left\lfloor \frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rfloor - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil = 0 \tag{2}$$

がすべての$\mathfrak{p}$について成り立つことをいう．仮定から$e_{\mathfrak{p}}-1=t_{\mathfrak{p}}$ ((1) 参照). また補題1(の証明)により$e_{\mathfrak{p}}=1$の場合は明らか． $m_{\mathfrak{p}}$は$\mathrm{mod}\ e_{\mathfrak{p}}$で按配してもよい．さらに$m_{\mathfrak{p}}=0$の場合は明らか．要するに算術の問題：

$$0<m<e \implies \left\lfloor \frac{m+e-1}{e} \right\rfloor = \left\lceil \frac{m}{e} \right\rceil \tag{3}$$

ができればよい．まず$0<\dfrac{m}{e}<1$より$\left\lceil \dfrac{m}{e} \right\rceil=0$. 次に$0 \leqq m-1<m<e$より$0 \leqq \dfrac{m-1}{e}<1$. よって$\left\lfloor \dfrac{m-1}{e} \right\rfloor=0$. したがって

$$\left\lfloor \frac{m+e-1}{e} \right\rfloor = \left\lfloor 1+\frac{m-1}{e} \right\rfloor = 1+\left\lfloor \frac{m-1}{e} \right\rfloor = 1+0=1$$

で万々歳．(証明終)

以下，本§ではK/kを代数体のガロア拡大，$G=\mathrm{Gal}(K/k)$とする．$\mathfrak{P}\,|\,\mathfrak{p}$なる$K,k$の素イデアル$\mathfrak{P},\mathfrak{p}$を用意する．$K_{\mathfrak{P}}$, $k_{\mathfrak{p}}$をそれぞれK,kの$\mathfrak{P},\mathfrak{p}$に関する完備化とすると$K_{\mathfrak{P}}/k_{\mathfrak{p}}$もガロア拡大で，§17，例1で述べたように$G_{\mathfrak{P}}=\mathrm{Gal}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$は$\mathfrak{P}$の$K/k$における分解群と同一視される．$K,k$の整数環$\mathcal{O}_K$, $\mathcal{O}_k$は自然に$K_{\mathfrak{P}}$, $k_{\mathfrak{p}}$の整数環$\mathcal{O}_{\mathfrak{P}}$, $\mathcal{O}_{\mathfrak{p}}$に埋め込まれる．単数群$\mathcal{O}_K{}^{\times}$, $\mathcal{O}_k{}^{\times}$についても同様である．コサイクル$c\in Z^1(G,\mathcal{O}_K{}^{\times})$は自然にコサイクル$c_{\mathfrak{P}}\in Z^1(G_{\mathfrak{P}},\mathcal{O}_{\mathfrak{P}}{}^{\times})$を定める．$\xi$を§22, (2)により$c$の定める$\mathcal{O}_K$の元とすれば，$\xi$を$\mathcal{O}_{K_{\mathfrak{P}}}$の元と見たものは$c_{\mathfrak{P}}$の定める元として通用する．

さて，

$$(4)\qquad \mathfrak{A}=(\xi)_K=\xi\mathcal{O}_K=\prod_{\mathfrak{p}}\mathfrak{p}^{\# m_{\mathfrak{p}}}$$

によってK/kに対して$m_{\mathfrak{p}}$が定まったのであるが，一方

$$(5)\qquad \mathfrak{A}_{\mathfrak{P}}=(\xi)_{K_{\mathfrak{P}}}=\xi\mathcal{O}_{\mathfrak{P}}=\mathfrak{P}^{m_{\mathfrak{P}}}$$

とおくと，

$$m_{\mathfrak{p}}=\nu_{\mathfrak{P}}(\mathfrak{A})=\nu_{\mathfrak{P}}(\mathfrak{A}_{\mathfrak{P}})=m_{\mathfrak{P}},\qquad \mathfrak{P}\,|\,\mathfrak{p}$$

が成り立つので，指数$m_{\mathfrak{p}}$は大局，局所の両方に通用する．事情は共役差積についても同様である：

$$(6)\qquad \mathcal{D}_{K/k}=\prod_{\mathfrak{p}}\mathfrak{p}^{\# t_{\mathfrak{p}}}=\prod_{\mathfrak{P}}\mathfrak{P}^{t_{\mathfrak{P}}}=\prod_{\mathfrak{P}}\mathcal{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

§22定理1，定理2はデデキント整域について一般に成り立ったのだから，K/kおよび$K_{\mathfrak{P}}/k_{\mathfrak{p}}$の場合に適用できる．このように局所化の視点からこれらの定理を積公式として書ける．

定理2　K/kを代数体のガロア拡大，$G=\mathrm{Gal}(K/k)$, $\mathfrak{P}\,|\,\mathfrak{p}$について$K_{\mathfrak{P}}/k_{\mathfrak{p}}$を$K/k$の局所化とする．このとき

$$\widehat{H}^0(G,\mathcal{O}_K{}^{+})_{\gamma}=\prod_{\mathfrak{p}}\widehat{H}^0(G_{\mathfrak{P}},\mathcal{O}_{\mathfrak{P}}{}^{+})_{\gamma_{\mathfrak{p}}},$$

ここに$\gamma\in H^1(G,\mathcal{O}_K{}^{\times})$に$\gamma_{\mathfrak{p}}\in H^1(G_{\mathfrak{P}},\mathcal{O}_{\mathfrak{P}}{}^{\times})$が対応する[6]．各$\mathfrak{p}$に対して

$$\widehat{H}^0(G_{\mathfrak{P}},\mathcal{O}_{\mathfrak{P}}{}^{+})_{\gamma_{\mathfrak{p}}}=\mathfrak{p}^{\left\lfloor\frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right\rfloor-\left\lceil\frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right\rceil}.$$

指数に関しては

$$i_\gamma(G,\ \mathcal{O}_K)=\prod_{\mathfrak{p}} i_{\gamma_\mathfrak{p}}(G_\mathfrak{P},\ \mathcal{O}_\mathfrak{P}).$$

各 $\mathfrak{p}$ に対して

$$i_{\gamma_\mathfrak{P}}(G_\mathfrak{P},\ \mathcal{O}_\mathfrak{P})=N\mathfrak{p}^{\left\lfloor\frac{m_\mathfrak{g}+t_\mathfrak{p}}{e_\mathfrak{p}}\right\rfloor-\left\lceil\frac{m_\mathfrak{p}}{e_\mathfrak{p}}\right\rceil}.$$

注意２　定理１によれば，$\mathfrak{P}$ が従順ならば $\prod_{\mathfrak{p}}$ の各成分は１である．したがって $\mathfrak{P}$ が野性的な場合の局所的考察だけが問題になる．

6）$\prod_{\mathfrak{p}}$の各成分にあらわれる $\mathfrak{P}$ は $\mathfrak{P}|\mathfrak{p}$ なるものを１つ選ぶことにする．ガロア拡大だから各成分の構造は $\mathfrak{P}$ のとり方によらない．以下同様．

第6話
局所体

24. 特性類

本話では k を $\mathfrak{p}$-進体とする(§15参照). K/k をガロア拡大, $G=\mathrm{Gal}(K/k)$, ガロア群, $\mathcal{O}_K$ を K の整数環, $\mathfrak{P}$ を $\mathcal{O}_K$ の(唯一の)素イデアル, $\mathfrak{P}=(\Pi)$, Π は1つの素元 $\in \mathcal{O}_K$, とする. 代数体の単数群は, ディリクレ(Dirichlet)の有名な単数定理はあるが, そのガロア群の作用によるコホモロジーはむずかしい. $\mathfrak{p}$-進体の場合には $H^1(G, \mathcal{O}_K{}^\times)$ は $e=e(K/k)$-次の巡回群としてきまる. これから定義する**特性類**とはこの巡回群の生成元 $\gamma_{K/k}$ のことである.

Π を上のように1つきめた $\mathcal{O}_K$ の素元とする. したがって

(1) $\quad {}^s\Pi=\Pi z_s, \qquad s \in G, \quad z_s \in \mathcal{O}_K{}^\times$

と書くことができる[1].

写像 $s \longmapsto z_s$ はコサイクル $z: G \to \mathcal{O}_K{}^\times$ である. 実際,

$$ {}^{st}\Pi=\Pi z_{st}={}^s({}^t\Pi)={}^s(\Pi z_t)={}^s\Pi{}^s z_t=\Pi z_s{}^s z_t, $$

よって

$$ z_{st}=z_s{}^s z_t. $$

1) 局所体では素イデアル $\mathfrak{P}$ はただ1つだから ${}^s\mathfrak{P}=\mathfrak{P}, s \in G$. さて ${}^s\mathfrak{P}={}^s(\Pi)=({}^s\Pi)=\mathfrak{P}=(\Pi)$ から (1) が出る.

次に Π' をもう 1 つの素元とすると ${}^s\Pi' = \Pi' z_s'$ によってコサイクル z' が定まるが，$\Pi' = \Pi u,\ u \in \mathcal{O}_K^{\times}$，とすれば

$$ {}^s\Pi' = {}^s\Pi\,{}^s u = \Pi z_s\,{}^s u = \Pi' z_s' = \Pi u z_s', $$

したがって

$$ z_s' = u^{-1} z_s\,{}^s u, $$

すなわち

$$ z' \sim z. $$

よって，$\gamma_{K/k} = [z]$ とおくと，これは K/k だけで定まるコホモロジー類になる．

定理 1　$H^1(G, \mathcal{O}_K^{\times}) = \langle \gamma_{K/k} \rangle.$

$$ |H^1(G, \mathcal{O}_K^{\times})| = e = e(K/k). $$

証明　$\gamma = [c]$ を $H^1(G, \mathcal{O}_K^{\times})$ の任意の元とする．$\mathcal{O}_K^{\times} \subset K^{\times}$ と考えると，ヒルベルト定理 90 により $\xi \in K^{\times}$ で

(2)　$$ c(s) = \xi^{-1}\,{}^s\xi $$

となるものがある．

(3)　$$ \xi = \Pi^m u, \qquad u \in \mathcal{O}_K^{\times}, m \in \mathbb{Z} $$

とかくと，(1) を用いて

(4)　$$ {}^s\xi = {}^s\Pi^m\,{}^s u = \Pi^m z_s^m\,{}^s u. $$

(2), (3), (4) から

(5)　$$ c(s) = u^{-1}\Pi^{-m}\Pi^m z_s^m\,{}^s u = u^{-1} z_s^m\,{}^s u $$

$$ \Longrightarrow \quad c \sim z^m \quad \Longrightarrow \quad \gamma = \gamma_{K/k}{}^m. $$

いいかえれば，$H^1(G, \mathcal{O}_K^{\times})$ は $\gamma_{K/k}$ の生成する巡回群になる．

次に，この群の位数を求める．まず短かい G-加群の完全系列：

(6)　$$ 1 \longrightarrow \mathcal{O}_K^{\times} \longrightarrow K^{\times} \longrightarrow \mathbb{Z} \longrightarrow 1, $$

ここに $K^{\times} \longrightarrow \mathbb{Z}$ は位数関数 ν_K を考える[2)]．(6) の定める長い完全系列(の一部分)を書くと：

(7)　$$ 1 \longrightarrow \mathcal{O}_k^{\times} \longrightarrow k^{\times} \longrightarrow \mathbb{Z} \longrightarrow H^1(G, \mathcal{O}_K^{\times}) \longrightarrow H^1(G, K^{\times}) = 1. $$

2）　G の $\mathbb{Z}$ への作用は trivial とする，i.e. ${}^s a = a,\ s \in G$.

ここで最後の等式はヒルベルト定理90による．さて，位数関数は $\nu_K(x)=e\nu_k(x), x\in k, e=e(K/k)$，を満足するから $\mathrm{Im}\, k^\times=e\mathbb{Z}$ で，(7) が完全であるから $H^1(G,\mathcal{O}_K{}^\times)\approx\mathbb{Z}/e\mathbb{Z}$．（証明終）

注意 1　§22，定理1で $c(s)=\xi^{-1}\,{}^s\xi$ の ξ を用いて不動イデアル

$$(\xi)=\prod_{\mathfrak{p}}\mathfrak{p}^{\#m_{\mathfrak{p}}}$$

と素因子分解した．ここに現れる $m_{\mathfrak{p}}$ と本§の (3) で用いた m は実は同じものである．少し正確にいうと，

(8)　$m_{\mathfrak{p}}\equiv m \pmod{e}.$

実際，$\gamma=[c]\sim\gamma_{K/k}{}^m$ から (1), (2), (5) によって

(9)　$c(s)=\xi^{-1}\,{}^s\xi=u^{-1}(\Pi^{-1}\,{}^s\Pi)^m\,{}^su,\qquad u\in\mathcal{O}_K{}^\times$

が出るから，(9) の第二の等式を

(10)　${}^s(\xi^{-1}u\Pi^m)=\xi^{-1}u\Pi^m$

と書けば，(10) の元は $k^\times$ に入る．したがって

(11)　$u\Pi^m=\xi v\pi^r,$

$v\in\mathcal{O}_k{}^\times, r\in\mathbb{Z}, \pi$ は $\mathcal{O}_k$ の素元，が成り立つ．(11) の両辺の $\nu_{\mathfrak{P}}$ をとって $\nu_{\mathfrak{P}}(\pi)=e$ を用いると，$\nu_{\mathfrak{P}}(\xi)=m_{\mathfrak{p}}$ だから

(12)　$m=m_{\mathfrak{p}}+re\equiv m_{\mathfrak{p}}\pmod{e}$

で (8) が証明された．

注意 2　$H^1(G,\mathcal{O}_K{}^\times)=\langle\gamma_{K/k}\rangle,\qquad \gamma_{K/k}{}^e=1$

により，任意の $\gamma=\gamma_{K/k}{}^m$，$0\leqq m\leqq e-1$，に対応する $\hat{H}^0(G,\mathcal{O}_K{}^+)_\gamma$ の構造は§22定理1ないし定理2によって

(13)　$\hat{H}^0(G,\mathcal{O}_K{}^+)_\gamma=\mathfrak{p}^{\left\lfloor\frac{m+t}{e}\right\rfloor-\left\lceil\frac{m}{e}\right\rceil},\qquad \gamma=\gamma_{K/k}{}^m,\qquad \mathfrak{D}_{K/k}=\mathfrak{P}^t.$

(14)　$i_\gamma(G,\mathcal{O}_K)=N\mathfrak{p}^{\left\lfloor\frac{m+t}{e}\right\rfloor-\left\lceil\frac{m}{e}\right\rceil}.$

K/k が従順な場合は任意の γ に対して $\hat{H}^0(G,\mathcal{O}_K{}^+)_\gamma=0, i_\gamma(G,\mathcal{O}_K)=1$ (§23定理1)であった．したがって野性的な場合($t\geqq e\geqq 2$)が残る．m の方は $\mathrm{mod}\, e$ で代えてよいから $0\leqq m\leqq e-1$．よって

(15) $$\left\lceil \frac{m}{e} \right\rceil = \begin{cases} 0, & m = 0, \\ 1, & m > 0. \end{cases}$$

したがって，$\gamma = 1\,(\Longleftrightarrow m = 0)$ のとき

(16) $$\hat{H}^0(G, \mathcal{O}_K{}^+)_1 = \mathfrak{p}^{\lfloor \frac{t}{e} \rfloor}, \qquad i_1(G, \mathcal{O}_K) = N\mathfrak{p}^{\lfloor \frac{t}{e} \rfloor} > 1.$$

また $\gamma \neq 1\,(\Longleftrightarrow m > 0)$ のとき

(17) $$\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma = \mathfrak{p}^{\lfloor \frac{m+t}{e} \rfloor - 1}, \qquad i_\gamma(G, \mathcal{O}_K) = N\mathfrak{p}^{\lfloor \frac{m+t}{e} \rfloor - 1}$$

となる．

とくに，$\gamma \neq 1$ のとき

(18) $$\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma \begin{cases} = 0, & m+t < 2e, \\ \neq 0, & m+t \geqq 2e \end{cases}$$

等々の結果が出る．

§ 25．共役差積と微分

局所体で便利なことは，共役差積 $\mathfrak{D}_{K/k}$ と K/k の最小多項式 $f(X)$ の微分 $f'(X)$ との間に極めてわかりやすい関係が存在することである．

定理 1 局所体の有限次拡大 K/k に対して $\theta \in K$ で $1, \theta, \cdots, \theta^{n-1}, n = [K:k]$ が $\mathcal{O}_K$ の $\mathcal{O}_k$ 上の自由底になるようなものが存在する．とくに $\mathcal{O}_K = \mathcal{O}_k[\theta]$ となる．$f(X)$ を θ の k 上の最小多項式とすると

$$\mathfrak{D}_{K/k} = (f'(\theta))$$

が成り立つ．したがって $\mathfrak{D}_{K/k} = \mathfrak{P}^t$ とすれば

$$t = \nu_{\mathfrak{P}}(f'(\theta))$$

である．

定義 1 多項式 $f(X) \in k[X]$ がアイゼンシュタイン多項式であるとは，$\mathfrak{p}$

を k の素イデアルとして

$$f(X) = X^m + a_{m-1}X^{m-1} + \cdots + a_1X + a_0$$

で $\mathfrak{p} \| a_0, \mathfrak{p} \mid a_1, \cdots, \mathfrak{p} \mid a_{m-1}$ が成り立つことをいう．

定理 2 アイゼンシュタイン多項式は k 上既約である．θ を $f(X)$ の根とし，$K = k(\theta)$ とすれば，K/k は**完全分岐**で $\nu_{\mathfrak{P}}(\theta) = 1$，すなわち θ は $\mathcal{O}_K$ の素元である．

逆に，K/k が完全分岐で Π を $\mathcal{O}_K$ の素元とすれば，Π の最小多項式はアイゼンシュタイン多項式で，

$$\mathcal{O}_K = \mathcal{O}_k[\Pi], \qquad K = k(\Pi)$$

が成り立つ．

例 1 $\quad f(X) = X^e - a \in \mathcal{O}_k[X], \qquad \nu_{\mathfrak{p}}(a) = 1$

はアイゼンシュタイン多項式である．定理 2 により $f(X)$ は k 上既約で，$f(\Pi) = 0$ とすると $K = k(\Pi)$ は完全分岐である．Π は $\mathcal{O}_K$ の素元になる．K/k をガロアにするために k は 1 の e 乗根を含むと仮定する．

さて，定理 1 より共役差積は

(1) $\qquad \mathcal{D}_{K/k} = (f'(\Pi)) = (e\Pi^{e-1})$

となる．さらに

(2) $\qquad t = \nu_{\mathfrak{P}}(f'(\Pi)) = e\nu_{\mathfrak{p}}(e) + (e-1),$

(3) $\qquad \mathcal{D}_{K/k} = \mathfrak{P}^t$

という関係にある．したがって §23,(1) より

(4) $\qquad K/k$ が従順 $\iff \nu_{\mathfrak{p}}(e) = 0$

である．この場合は

$$\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma = 0, \qquad i_\gamma(G, \mathcal{O}_K) = 1$$

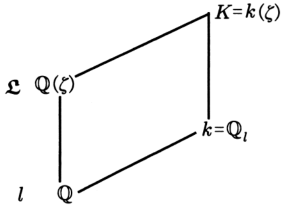
であった(§23，定理 1)．$\nu_{\mathfrak{p}}(e) \geqq 1$ の場合は拡大は野性的で，(2) を §24 (17) に代入することにより $\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma$，$i_\gamma(G, \mathcal{O}_K)$ が定まる．ただし，$\gamma = \gamma_{K/k}{}^m$，$0 \leqq m \leqq e-1$ であった．

注意 1 例 1 の K/k はいわゆるクンマー体である：$K = k(\sqrt[e]{a})$.

例 2 (円の l^n 分体) $\quad n \geqq 1$，l を素数，ζ を 1 の原始 l^n 乗根とする．たと

えば $\zeta = e^{\frac{2\pi i}{l^n}}$．このとき $\mathbb{Q}(\zeta)/\mathbb{Q}$ は次数 $\varphi(l^n) = l^{n-1}(l-1)$ のガロア拡大体で，ガロア群 $G \approx (\mathbb{Z}/l^n\mathbb{Z})^\times$ である．$\mathbb{Q}(\zeta)/\mathbb{Q}$ で分岐する $\mathbb{Q}$ の素数は l のみで，それは完全分岐する．l の $\mathbb{Q}(\zeta)$ における分解は

(5)　　$l = \mathfrak{L}^e, \qquad e = \varphi(l^m), \quad \mathfrak{L} = (1-\zeta)$



拡大 $\mathbb{Q}(\zeta)/\mathbb{Q}$ を素イデアル $l, \mathfrak{L}$ について局所化して K/k, $k = \mathbb{Q}_l$, $K = k(\zeta)$ を得るが，$\mathfrak{L}$ は完全分岐するからその分解体は $\mathbb{Q}$ で局所化しても

$$[K:k] = e = \varphi(l^n), \qquad G = \mathrm{Gal}(K/k) \approx (\mathbb{Z}/l^n\mathbb{Z})^\times$$

と変化がない．l 以外の任意の素イデアルは不分岐だから

(6)　　$\mathscr{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathscr{D}_{K/k}$

である．一方，円分体で知られているように

(7)　　$\mathscr{D}_{\mathbb{Q}(\zeta)/\mathbb{Q}} = \mathfrak{L}^t, \qquad t = n\varphi(l^n) - l^{n-1}$

だから，(6), (7) より

(8)　　$\mathscr{D}_{K/k} = \mathfrak{L}^t, \qquad t = n\varphi(l^n) - l^{n-1} = l^{n-1}(n(l-1)-1)$

を得る．したがって $\gamma = {\gamma_{K/k}}^m$, $0 \leqq m \leqq e-1$ の m と $e = \varphi(l^n)$ と (8) の t によって $\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma$ ないし $i_\gamma(G, \mathcal{O}_K)$ を $\gamma \in H^1(G, \mathcal{O}_K{}^\times)$ について決定することができる．とくに $m = 1$ の場合，すなわち $\gamma = \gamma_{K/k}$，特性類，の場合である．$\gamma_{K/k} = [c]$ とすると § 24，(2), (3) から

(9)　　$c(s) = \Pi^{-1s}\Pi, \qquad \Pi = 1-\zeta$

にとることができる．$\mathfrak{L} = (1-\zeta)$ は素な不動単項イデアルだから $\Pi = 1-\zeta$ がベストの選択である[3]．まず (8) より

(10)　　$t = ne - l^{n-1}, \qquad n \geqq 1.$

さて，K/k が従順であることは $t = e-1$ あるいは $l \nmid e$ と同値であるが，

3）§ 4，注意 1 で触れたように，(9) の $c(s)$, $s \in G$ はいわゆる円単数である．その類が特性類である．

この判別法により

(11) $\quad K/k$ が従順 $\iff n=1$

を得る．実際 $n=1$ なら (10) により明らか．また $n \geqq 2$ ならば (10) から，もし K/k が従順ならば $ne-l^{n-1}=e-1$，よって $(n-1)l^{n-1}(l-1)=l^{n-1}-1$ で $l|1$ となり不可能である．つまり K/k は野性的になる．そこで $n \geqq 2$ とする．すると $t \geqq e \geqq 2$ で，

(12) $\quad n-1 < \dfrac{t+1}{e} < n$

が成り立つことが確かめられる．(12) の各項を e 倍して

(13) $\quad en-e < t+1 < en$

をいえばよいが，(8) から $t=ne-l^{n-1}$ だから，これを (13) に入れて簡略すれば

(14) $\quad e > l^{n-1}-1 > 0$

が証明すべき式になるが，$e=l^{n-1}(l-1)$ だから $n \geqq 2, l \geqq 2$ なる限り (14) は O.K. (12) をいいかえれば

(15) $\quad n \geqq 2$ のとき $\left\lfloor \dfrac{t+1}{e} \right\rfloor = n-1.$

§ 24，(17) によれば，$m=1$ として

$$\begin{cases} \widehat{H}^0(G, \mathcal{O}_K{}^+)_{\gamma_{K/k}} = (l\mathbb{Z})^{\left\lfloor \frac{t+1}{e} \right\rfloor - 1}, \\ i_{\gamma_{K/k}}(G, \mathcal{O}_K) = l^{\left\lfloor \frac{t+1}{e} \right\rfloor - 1} \end{cases}$$

であるから，これに(15)を代入して，次の命題を得る．

命題 1 $\quad n \geqq 2$ のとき K/k，$k=\mathbb{Q}_l$，$K=k(\zeta)$，$\zeta=1$ の原始 l^n 乗根，は野性的拡大で

$$\begin{cases} \widehat{H}^0(G, \mathcal{O}_K{}^+)_{\gamma_{K/k}} = (l\mathbb{Z})^{n-2}, \\ i_{\gamma_{K/k}}(G, \mathcal{O}_K) = l^{n-2}. \end{cases}$$

注意 2 $\quad n=2$ とすると，命題 1 の右辺は 0 または 1 となって消えてしまう．これは拡大が野性的であってもコホモロジーないし指数が消滅する例である．

第7話
2次体再訪

§26. 問題の再記(2次体の場合)

d を平方因子をふくまない整数とし，$K=\mathbb{Q}(\sqrt{d})$ を2次体とする[1]．p を素数，$\mathfrak{P}$ を p を割る K の素イデアル，$\mathbb{Q}_p$，$K_\mathfrak{P}$ をそれぞれ $p, \mathfrak{P}$ に関する $\mathbb{Q}$，K の完備化(あるいは局所化)とする．したがって $K_\mathfrak{P}=\mathbb{Q}_p(\sqrt{d})$ は高々2次である．$[K_\mathfrak{P}:\mathbb{Q}_p]=1$，すなわち $d\in\mathbb{Q}_p^{\times 2}$ の場合は

$$G=\mathrm{Gal}(K_\mathfrak{P}/\mathbb{Q}_p)=1$$

で，何も問題はない．

命題1

$$K_\mathfrak{P}=\mathbb{Q}_p \iff \begin{cases} p\nmid d,\ \left(\dfrac{d}{p}\right)=1, & p\neq 2\ \text{のとき}, \\ 2\nmid d,\ d\equiv 1\ (\mathrm{mod}\ 8), & p=2\ \text{のとき}. \end{cases}$$

われわれはこの命題1の場合に興味はないのだから，両辺を否定した命題を明示すると，

1) 第3話では d の代りに m を用いていたが，第5話以降で m は別の意味に用いたので，ここでは d を用いることにする．

命題 2

$$[K_{\mathfrak{P}}:\mathbb{Q}_p]=2 \iff \begin{cases} p\,|\,d \quad \text{または} \quad p \nmid d \text{ で} \left(\dfrac{d}{p}\right)=-1, \\ \hfill p\neq 2 \text{ のとき}, \\ 2\,|\,d \quad \text{または} \quad d\equiv 3,5,7 \pmod 8, \\ \hfill p=2 \text{ のとき}. \end{cases}$$

となる．

次に K の判別式 D_K について，

命題 3 $K=\mathbb{Q}(\sqrt{d})$,

$$D_K=\begin{cases} 4d, & d\equiv 2,3 \pmod 4, \\ d, & d\equiv 1 \pmod 4). \end{cases}$$

そこで $[K_{\mathfrak{P}}:\mathbb{Q}_p]=2$ となる p を分類すると命題 2，命題 3 から

$$(1) \qquad \begin{cases} p\,|\,D_K \\ [K_{\mathfrak{P}}:\mathbb{Q}_p]=2 \end{cases} \iff \begin{cases} p\,|\,d, & p\neq 2, \\ d\equiv 2,3 \pmod 4, & p=2 \end{cases}$$

となる．ついでながら

$$(2) \qquad \begin{cases} p\nmid D_K \\ [K_{\mathfrak{P}}:\mathbb{Q}_p]=2 \end{cases} \iff \begin{cases} p\nmid d, & p\neq 2, \\ d\equiv 1 \pmod 4), & p=2. \end{cases}$$

とにかく $p\nmid D_K$ ならば $K_{\mathfrak{P}}/\mathbb{Q}_p$ は不分岐だから，何も問題は起こらない．

さらに $p\,|\,D_K$ で $p\neq 2$ の場合(したがって $p\,|\,d$)，p は分岐する，すなわち $p=\mathfrak{P}^2$ であるが，$e=2$ で $p\neq 2$ だから $p\nmid e$．よって $K_{\mathfrak{P}}/\mathbb{Q}_p$ は従順である．したがって，最後に残るのは (1) により，$p=2\,|\,D_K=4d$ かつ $d\equiv 2,3 \pmod 4$ の場合になる．この場合には $e=2, p=2$ だから $p\,|\,e$，よって拡大 $K_{\mathfrak{P}}/\mathbb{Q}_p$ は野性的である．このように野性的な素数は $p=2$ ただ 1 つになり，§23 定理 2 の大局的なコホモロジーの決定は $p=2$ における局所的コホモロジーの決定に他ならないことになる．これを次の § で実行しよう．

§27. 問題の解決

$K=\mathbb{Q}(\sqrt{d})$ を2次体．$G=\mathrm{Gal}(K/\mathbb{Q})=\langle s\rangle$．§23 定理2によって

(1) $$\hat{H}^0(G, \mathcal{O}_K{}^+)_\gamma=\hat{H}^0(G, \mathcal{O}_{\mathfrak{P}}{}^+)_{\gamma_{\mathfrak{P}}},$$

ここに $\mathfrak{P}\,|\,2$ (実は $2=\mathfrak{P}^2, e=2$)，$\gamma\in H^1(G, \mathcal{O}_K{}^\times)$，そして $\gamma_{\mathfrak{P}}$ は γ の定める $H^1(G, \mathcal{O}_{\mathfrak{P}}{}^\times)$ のコホモロジー類[2)]．さらに同定理によって

(2) $$\begin{cases}\hat{H}^0(G, \mathcal{O}_{\mathfrak{P}}{}^+)_{\gamma_{\mathfrak{P}}}\approx(2\mathbb{Z})^{\left\lfloor\frac{m_2+t_2}{2}\right\rfloor-\left\lceil\frac{m_2}{2}\right\rceil}, \\ i_{\gamma_{\mathfrak{P}}}(G, \mathcal{O}_{\mathfrak{P}})=2^{\left\lfloor\frac{m_2+t_2}{2}\right\rfloor-\left\lceil\frac{m_2}{2}\right\rceil}.\end{cases}$$

注意1　2次体の場合 $e=2$ で m_2 は $0\leqq m_2\leqq e-1=1$ にとれたから，m_2 は本質的に0か1である．$\gamma_{\mathfrak{P}}=\gamma_{K_{\mathfrak{P}}/\mathbb{Q}_2}{}^{m_2}$, $H_1(G, \mathcal{O}_{K_{\mathfrak{P}}}{}^\times)=\langle\gamma_{K_{\mathfrak{P}}/\mathbb{Q}_2}\rangle$ は位数 $=2$ であった(§24，定理1)から，$\gamma_{\mathfrak{P}}$ も1か $\gamma_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ の2つしかなく，それぞれ m_2 の丁半に対応する．これが第3話の丁半の問題に他ならない．それには t_2 をはっきりさせないといけない．ここに t_2 は

$$\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_2}=\mathfrak{P}^{t_2}$$

で定まっていた．したがって $\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_2}$ を決めねばならない．(注意終)

§26 の終り近くで述べたように，$p=2, d\equiv 2, 3 \pmod 4$ の場合が問題であった．

第1の場合　$p=2, d\equiv 2 \pmod 4$.

$f(X)=X^2-d\in\mathbb{Q}_2[X]$ は $\sqrt{d}$ の $\mathbb{Q}_2$ 上の最小多項式で，$2\,\|\,d$ だからアイゼンシュタイン多項式である．§25 定理2から $\Pi=\sqrt{d}$ は $\mathcal{O}_{\mathfrak{P}}$ の素元で

(3) $$\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_2}=(f'(\Pi)).$$

$f'(\Pi)=2\Pi$．一方，$\Pi^2=d=2(1+2k)$ で $1+2k$ は2-単数だから $\Pi^2\sim 2$[3)]．よって $f'(\Pi)\sim\Pi^3$．これを(3)に入れて

(4) $$\mathcal{D}_{K_{\mathfrak{P}}/\mathbb{Q}_2}=\mathfrak{P}^3, \qquad t_2=3.$$

2） $G_{\mathfrak{P}}=G=\langle s\rangle$ に注意．

3） $\mathbb{Q}_2{}^\times$ で $a\sim b$ は a と b が $\mathbb{Z}_2{}^\times$ を除いて等しいことを表わす．

これで e, t_2 がきまり，m_2 は注意 1 のように $\gamma_{\mathfrak{P}}$ の $=1, \neq 1$ に応じて $m_2=0$, 1 となるので (2) (の指数 $i_{\gamma_{\mathfrak{P}}}$ の方だけ書くことにして),

$$(5)\qquad \begin{cases} i_1 = 2^{\left\lfloor \frac{t_2}{e} \right\rfloor} = 2^{\left\lfloor \frac{3}{2} \right\rfloor} = 2, \\ i_{\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2}} = 2^{\left\lfloor \frac{t_2+1}{e} \right\rfloor - \left\lceil \frac{1}{e} \right\rceil} = 2^{\left\lfloor \frac{3+1}{2} \right\rfloor -1} = 2 \end{cases}$$

を得る．

第 2 の場合　$p=2, d\equiv 3 \pmod 4$.

このとき $f(X)=X^2-d$ は d が奇数なのでアイゼンシュタイン多項式ではないが，$X \longmapsto X-1$ と変数変換すると

$$g(X)=f(X-1)=(X-1)^2-d=X^2-2X+(1-d)$$

は $2 \| (1-d)$ なのでアイゼンシュタイン多項式になる．$\Pi=\sqrt{d}+1$ とおくと，これは $g(\Pi)=0$ を満足するから $\mathcal{O}_{\mathfrak{P}}$ の素元になる．よって

$$(6)\qquad \mathcal{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2}=(g'(\Pi)).$$

$g'(\Pi)=2\Pi-2=2(\Pi-1)=2\sqrt{d}\sim 2\sim \Pi^2$ より

$$(7)\qquad \mathcal{D}_{K_{\mathfrak{P}}/\mathbf{Q}_2}=\mathfrak{P}^2, \qquad t_2=2.$$

そして

$$(8)\qquad \begin{cases} i_1 = 2^{\left\lfloor \frac{t_2}{e} \right\rfloor} = 2, \\ i_{\gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2}} = 2^{\left\lfloor \frac{t_2+1}{e} \right\rfloor - \left\lceil \frac{1}{e} \right\rceil} = 2^{\left\lfloor \frac{3}{2} \right\rfloor -1} = 1. \end{cases}$$

注意 2　ここで第 3 話との連絡をつけておこう．実 2 次体 $K=\mathbf{Q}(\sqrt{d})$[4] のコサイクル類 $\gamma=[\varepsilon]$，ε は $N\varepsilon=1$ なる基本単数[5]，に対して $i_\gamma=i_\gamma(G, \mathcal{O}_K)$ が定まるが[6],

(I)　$d\equiv 1 \pmod 4$ ならば　$i_\gamma=1$.

(II)　$d\equiv 2 \pmod 4$ ならば　$i_\gamma=2$.

(III)　$d\equiv 3 \pmod 4$ のとき

$$a_s\equiv 1 \pmod 2 \Longrightarrow i_\gamma=1,$$
$$a_s\equiv 0 \pmod 2 \Longrightarrow i_\gamma=2$$

---

4)　この d は第 3 話の m.

5)　ε はコサイクルと同一視されていた(§8, (4) 参照).

6)　§9 の注意 1 参照.

が証明されていた．一方，$\gamma = [\varepsilon]$ に対して

$$(9) \qquad i_\gamma(G, \mathcal{O}_K) = i_{\gamma_{\mathfrak{P}}}(G, \mathcal{O}_{\mathfrak{P}}), \qquad \mathfrak{P}|2.$$

そして $d \equiv 1\ (4)$ ならば $K_{\mathfrak{P}}/\mathbf{Q}_2$ は不分岐．また $d \equiv 2\ (4)$ ならば $i_\gamma, i_{\gamma_{\mathfrak{P}}}$ は常に $= 2$，最後に $d \equiv 3\ (4)$ ならば

$$(10) \qquad a_s \equiv 0 \pmod 2 \iff i_\gamma = 2 = i_{\gamma_{\mathfrak{P}}} \iff \gamma_{\mathfrak{P}} = \gamma_{K_{\mathfrak{P}}/\mathbf{Q}_2} \neq 1,$$

$$(11) \qquad a_s \equiv 1 \pmod 2 \iff i_\gamma = 1 = i_{\gamma_{\mathfrak{P}}} \iff \gamma_{\mathfrak{P}} = 1$$

となって話の辻褄があう．

もちろん連分数など一般の代数的整数論から見れば実2次体においてのみ意味を持つものであるが，§23の一般的定理1，定理2のような見透しよい結果も実2次体における実験なしには(筆者には)到達できなかったのも事実である．

参考文献

[A] 浅野啓三：環論及びイデアル論，共立社，1949

[C&F] J. W. S. Cassels & A. Frölich (Ed.) : Algebraic Number Theory, Academic Press, 1967

[D] M. Deuring : Algebren, Springer, 1968

[F] 藤崎源二郎：代数的整数論 (上), (下)，裳華房，1975

[G] R. C. Gunning : Lectures on Modular Forms, Princeton, 1962

[H] D. Hilbert : Die Theorie der algebraischen Zahlkörper (Zahlbericht), 1897

[K] M. Kneser : Lectures on Galois Cohomology of Classical Groups, Tata Institute, 1969

[L] S. Lang : Algebra, Springer, 2002

[L&O] S.-M. Lee & T. Ono : On a certain invariant for real quadratic fields, Proc. Japan Acad. Vol. 79 (2003), 119-122

[O] 小野孝：数論序説，裳華房，2001

[O_2] T. Ono : A note on Poincaré sums for finite groups, Proc. Japan Acad. vol. 79 (2003), 95-97

[O_3] T. Ono : On Poincaré sums for local fields, Proc. Japan Acad. vol. 79 (2003), 115-118

[O_4] T. Ono : On Poincaré sums for number fields, Proc. Japan Acad. vol. 81 (2005), 65-68

[P] H. Poincaré : Mémoire sur les fonctions fuchsiennes, Acta Math. 1 (1882), 193-294

[R] C. Reid : Hilbert, Springer, 1970

[S] J.-P. Serre : A course in Arithmetic, Springer, 1973

[S_2] J.-P. Serre : Galois Cohomology, Springer, 1994

[Sh] I. R. Shafarevich, Basic Algebraic Geometry, Springer, 1974

[St] H. M. Stark : An Introduction to Number Theoy, MIT Press, 1978

[T] 高木貞治：代数的整数論，岩波書店，1971

付録

付録1
整数論 = 素数論

私に与えられたこの表題にはじめは少々抵抗を感じたのですが，それが私にいろいろ考えるヒントを与えたことも事実で，今ではむしろ有難いことと思っています．以下，整数論と素数について思いつくまま書いて見ます．読者と私との共通の典拠として「初整」として『初等整数論講義』(共立出版)，「解概」として『解析概論』(岩波書店)を引用します．いずれもご存知の高木貞治先生の本です．また岩波書店の『岩波数学辞典(第3版)』も便利ですから「辞典」として引用します．

§1．素数

「初整」で素数があらわれるのは§4，p. 11で，それまでは素数を使わずに整数の整除(§1)，最大公約数，最小公倍数(§2)，一次不定方程式(§3)が論じられています．開き直って，素数なしでどのくらい整数論ができるかというと，たとえば「初整，第2章，連分数」がそれで，これは立派な整数論です[1]．私が表題に抵抗を感じたと書いたのはこのようなことだったのです．しかし整数論の基本定理(素因数分解の可能性と一意性，「初整，p.12」)が整数論で基本的なことは確かですから，標題の等号は大目に見るのがよいでしょう．

「初整，p. 20」に**素数の数は無限にある**がユークリッドの例の方法で証明されています．また開き直って，素数が無限にあることを使わないで証明できる定理はと問えば，こんどは「初整」の大部分の定理が出てきます．このごろはやりの素数と素粒子の対比にあやかれば，素粒子が無限にあることを証明(仮定？)しなくても十分物理を展開できるのと同じようなことなのでしょうか？

しかし，こと数学に関する限り，もしも素数が有限個しかなかったら整数論はまことに淋しいものでしょう．これはディリクレの算術級数定理(「初整，p. 385」)とその後世への影響を考えてみればわかります．

ディリクレの定理は

‘互いに素な自然数 a, m が与えられたとき 1 次式

$$f(x) = a+mx$$

が無数の素数をあらわす’

を主張します[2)]．1 次式を 2 つ考えて，

$$f(x) = x, \qquad g(x) = x+2$$

とし，両方が同時に素数になるような x が無限にあるかというのが**双子の素数**の問題で，また

$$f(x) = x, \qquad g(x) = 2x+1$$

の場合が**ソフィー・ジェルマンの素数**の問題です．いずれも今のところ未解決のようです．

非線型の場合，$f(x) = x^2+1$ が無限に素数をあらわすかどうかもわかっていないと思います．有名なのは

$$f(x) = 2^x+1 \qquad (\text{フェルマ}),$$

$$f(x) = 2^x-1 \qquad (\text{メルセンヌ})$$

の場合で，計算機が良くなるごとにずいぶん大きな x について実験できるようで，フェルマの場合には有限個の素数しかあらわれない，メルセンヌの場合には無限個あらわれると予想されています．一般に奇数 $z \geqq 3$ は

$$z = f(x, y) = 1+2^x y, \qquad x, y \geqq 1, \quad y \text{ は奇数},$$

と一意的に書けますが，z が素数となる条件を x, y で記述できるでしょうか？　フェルマの素数は $y = 1$ のときです[3)]．

未解決の問題を並べましたが，ここで素数が無数にあることを証明する他の

方法に目を転ずることにしましょう．「解概，pp. 179-180」により，$s>1$ のとき

(1)　$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}$$　（リーマンのゼータ関数）

は収束し，積展開

(2)　$$\zeta(s)=\prod_{p}\frac{1}{1-p^{-s}}$$　（オイラーの等式）

が成り立ちます．ここで p はすべての素数をわたるのですが，必要なことがらは整数論の基本定理だけで，素数が有限か無限かは関係ありません．一方「解概，p. 236」により

(3)　$$\zeta(2)=\frac{\pi^2}{6}$$

が成り立ちます．これには (1) だけが必要で，(3) は素数とは無関係な解析の命題です．さて，(2), (3) から

(4)　$$\frac{\pi^2}{6}=\prod_{p}\frac{1}{1-p^{-2}}$$

が出ますから，もし p が有限個しかなければ (4) の右辺が有理数で，したがって π^2 が有理数で，π が超越数であることに矛盾します[4)]．ここで大事なことは (4) が単に素数が無限にあること以上のものを含んでいることです．円周率 π は円から来たものですから，(4) は，大げさにいえば，

(5)　幾何 ＝ 整数論

と見ることもできましょう．一方，これも大げさ過ぎますが，

(6)　幾何 ＝ 物理

といったことも支持されることがあるようで，(5), (6) から‘幾何’を消去すれば……．このエッセイで私がいいたいのは，(4) があとに述べる‘アデール幾何’における等式の特殊な場合と考えられるということです．ですから，(5) は大げさではあってもそれほど荒唐無稽なものではないのです．

§2. アデール

素数を

(7)　　$2, 3, 5, 7, 11, 13, 17, \cdots$

と大きさの順に並べると無限に続くのですが，記号 ∞ を導入すると，(7) は

(8)　　$2, 3, 5, 7, 11, 13, 17, \cdots, \infty$

と完結します．∞ のことを**無限素点**とよび，通常の素数 p を**有限素点**とよびます．さらに p と ∞ をひっくるめて v と書いて**素点**とよびます．

有限素点(すなわち素数)の全体を P，素点の全体を $\hat{P}$ と書きましょう．したがって

$$\hat{P} = P \cup \{\infty\}$$

です．通常の複素平面 $\mathbb{C}$ に無限遠点 ∞ を加えて $\hat{\mathbb{C}}$ とすると，$\hat{\mathbb{C}}$ は球面と同一視され ∞ は北極に対応することはご存知の通りですが，整数論の場合も同様に考えます．$\mathbb{C}$ を $\hat{\mathbb{C}}$ に拡張することにより，すなわち $\mathbb{C}$ に ∞ を加えるコンパクト化により複素関数論が明快になるように，P を $\hat{P}$ に拡張することにより整数論が明快になるだろうと考えるのは自然です．

このように，有理数体 $\mathbb{Q}$ の局所化として各素点 $v \in \hat{P}$ に対して局所体 $\mathbb{Q}_v$ が，$\mathbb{Q}$ の絶対値 $|\ \ |_v$ の定める距離に関する完備化として得られるのです．すなわち，$v = \infty$ のときは

$$|a|_\infty = |a| \qquad (\text{有理数 } a \text{ の通常の絶対値}),$$

$v = p$ のときは

$$|0|_p = 0,$$

また $a \neq 0$ のとき $a = p^e b$，b の分母子は p と素，としたとき

$$|a|_p = p^{-e}$$

として定義されます．定義から直ちに

$$|a|_v = 0 \iff a = 0$$

(9)　　$|ab|_v = |a|_v |b|_v$

$$|a+b|_v \leqq |a|_v + |b|_v, \qquad a, b \in \mathbb{Q}$$

とくに

(10)　　$|a+b|_p \leqq \max(|a|_p, |b|_p)$

が成り立つことがわかります．そこで $\mathbb{Q}$ の 2 点 a, b の距離 $d_v(a, b)$ を

$$d_v(a, b) = |a-b|_v$$

で定義すると $\mathbb{Q}$ は距離空間となり，d_v による $\mathbb{Q}$ の完備化として完備な距離空間 $\mathbb{Q}_v$ が得られます[5]．$\mathbb{Q}_v$ もまた自然に体になり，

$$a = v\text{-}\lim_{n\to\infty} a_n \qquad (a_n \in \mathbb{Q})$$

のとき

$$|a|_v = \lim_{n\to\infty} |a_n|_v$$

により $\mathbb{Q}_v$ に絶対値 $|\ \ |_v$ が拡張され，それは (9), (10) の性質を持ちます．このようにして各 $v \in \hat{P}$ に対して局所体 $\mathbb{Q}_v$ が得られたわけですが，とくに $v = \infty$ のときは上の手続きはカントルの実数の定義そのままですから $\mathbb{Q}_\infty = \mathbb{R}$ (実数体)です．$\mathbb{Q}_p$ の方は p-進体とよばれます．

$\mathbb{Q}_p$ の部分集合

(11)　　$\mathbb{Z}_p = \{ a \in \mathbb{Q}_p ; |a|_p \leqq 1 \}$

は $\mathbb{Q}_p$ の部分環になります．これは $v = \infty$ のときの閉区間 $[-1, 1]$ の類似ですが，(10) という強い 3 角関係のために，単に $[-1, 1]$ のようにコンパクト集合であるばかりでなく，$\mathbb{Q}_p$ の加法について閉じているのです．$\mathbb{Z}_p$ は p-進整数環とよばれています．これで曲がりなりにもアデールを定義する道具が揃いました．

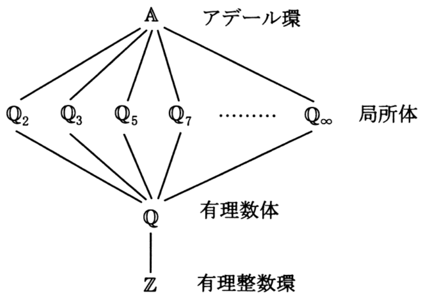
直積 $\prod_{v \in \hat{P}} \mathbb{Q}_v$ の要素 $a = (a_v)$ に対して

(12)　　$a = (a_v)$ がアデール

$$\overset{\text{定義}}{\Longleftrightarrow} \quad \text{有限個の } p \text{ を除いて } a_p \in \mathbb{Z}_p$$

とし，アデールの全体を $\mathbb{A}$ と書きます．$\mathbb{A}$ は自然に環となり，自然に位相が入り，有理数体 $\mathbb{Q}$ は対角写像 $a \longmapsto (a, a, \cdots, a, \cdots), a \in \mathbb{Q}$, により $\mathbb{A}$ の中の離散的な部分加群とみなされます．そして商群 $\mathbb{A}/\mathbb{Q}$ はコンパクトになりま

す[6)]．われわれは整数論のふるさとである $\mathbb{Z}$ ないし $\mathbb{Q}$ から出発し，複素関数論を手本にして，アデール環 $\mathbb{A}$ の概念に到達いたしました．



ここで，$\mathbb{Q}_\infty = \mathbb{R}$ は幾何，解析の場で，$\mathbb{Q}_p$ は整数論の場でありますから $\mathbb{A}$ は幾何，解析，整数論を一身に集め，か弱き数学の女王 $\mathbb{Z}$ を優しく包んでいるのでありましょう．

§3．玉河数

第1節の (4) の等式の 'アデール幾何' における意味を考えてみましょう．以下の説明で少々耳慣れない言葉や記号が出てくると思いますが，それは主に言葉の問題で，実質的にはオイラーあたりの数学(18世紀の数学)にいくらか群論の考察を加えたものですから，あまり細部や数式にこだわらずに気楽に読んでください．

［お手元に「辞典」がありましたらどんどん使ってください．「辞典」は第2次大戦以後の第一線の日本の数学者達により書きつがれてきたもので，これ1冊で各種教科書100冊分ぐらいの威力があります．］

第2節の

$$\mathbb{Q} \longrightarrow \mathbb{Q}_v\,(v \in \hat{P}) \longrightarrow \mathbb{A}$$

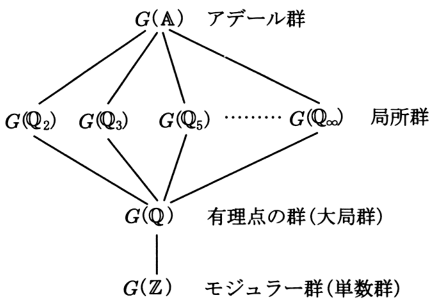
のプロセスは $\mathbb{Q}$ から出発するだけでなく，$\mathbb{Q}$ で定義された代数多様体 X に適用されます．X は $\mathbb{Q}$ を係数とするある多変数多項式の系の共通零点として与えられますから，その零点をとる体や環を変化させれば

$$X(\mathbb{Q}) \longrightarrow X(\mathbb{Q}_v)\,(v \in \hat{P}) \longrightarrow X(\mathbb{A})$$

のプロセスを考えられるわけで，このプロセスを X の($\mathbb{Q}$ に関する)アデール化とよびます．

もちろん，この途中で $X(\mathbb{Z}_p)$ も考えなければなりません．とくに X として 2 次の特殊線型群 $X = G = SL_2$ をとりますと

$$(13) \qquad G(\mathbb{Q}) = \left\{ x = \begin{pmatrix} t_1 & t_2 \\ t_3 & t_4 \end{pmatrix}; \det x = 1 \right\} \qquad \text{ただし } t_i \in \mathbb{Q},\ 1 \leqq i \leqq 4$$



となり，t_i のとる範囲を $\mathbb{Q}_v, \mathbb{Z}_p, \mathbb{A}$ に変えることにより $G(\mathbb{Q}_v), G(\mathbb{Z}_p), G(\mathbb{A})$ ができます．いちばん小さい $G(\mathbb{Z}) = SL_2(\mathbb{Z})$ がいわゆる(楕円)モジュラー群です．

$G = SL_2$ は 3 次元ですから，t_1, t_2, t_3 を G の単位元のまわりのパラメータと見て微分形式(体積要素)

$$(14) \qquad \omega = \frac{dt_1 \wedge dt_2 \wedge dt_3}{t_1}$$

を考えると，ω は G の左不変な微分形式になります．$\omega_{\mathbf{A}}$ を ω が $G(\mathbb{A})$ に定めるハール測度としたとき

(15) $$\tau(G)=\int_{G(\mathbb{Q})\backslash G(\mathbb{A})}\omega_{\mathbb{A}}$$

が G の**玉河数**です[7]．

これを計算してみましょう．

F を $G(\mathbb{Z})\backslash G(\mathbb{R})$ の基本領域とすると，G の類数 $=1$ となることから，$G(\mathbb{Q})\backslash G(\mathbb{A})$ の基本領域 $\tilde{F}$ は

(16) $$\tilde{F}=F\times\prod_{p\in P}G(\mathbb{Z}_p)$$

で与えられ，(15) の計算は

(17) $$\tau(G)=\int_F\omega_\infty\times\prod_p\int_{G(\mathbb{Z}_p)}\omega_p$$

と局所体に関する積分の計算に帰着します[8]．さて，1 つの素数 p に対して $G(\mathbb{Z}_p)$ の部分群

(18) $$G^{(1)}(\mathbb{Z}_p)=\left\{x=\begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix}\in G(\mathbb{Z}_p)\,;\begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix}\equiv\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\bmod p\right\}$$

を考えると，同型

(19) $$G(\mathbb{Z}_p)/G^{(1)}(\mathbb{Z}_p)\approx SL_2(\mathbb{F}_p),$$
$$\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$$

が得られ，右辺の有限群の位数が $p(p^2-1)$ となることから

(20) $$\int_{G(\mathbb{Z}_p)}\omega_p=p(p^2-1)\int_{G^{(1)}(\mathbb{Z}_p)}\omega_p=\frac{p(p^2-1)}{p^3}=1-p^{-2}$$

したがって (4) より

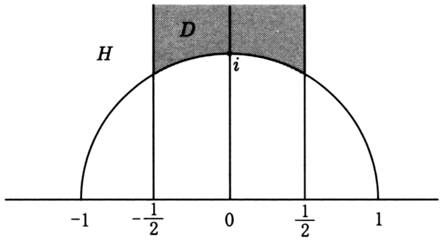
(21) $$\prod_p\int_{G(\mathbb{Z}_p)}\omega_p=\prod_p(1-p^{-2})=\frac{6}{\pi^2}$$

が出ました．これが整数論側の計算です．

次に ∞ すなわち幾何，解析側の計算ですが，これは古典理論のよい復習でしょう．まず，$G(\mathbb{R})=SL_2(\mathbb{R})$ は上半平面 $H=\{z\in\mathbb{C}\,;\mathrm{Im}\,z>0\}$ に

(22) $$x\cdot z=\frac{t_1z+t_2}{t_3z+t_4},\qquad x=\begin{pmatrix}t_1 & t_2\\ t_3 & t_4\end{pmatrix}\in G(\mathbb{R})$$

により推移的に作用し，$i=\sqrt{-1}$ における固定群は



(23)　　$K = \{ x \in G(\mathbb{R}) ; xi = i \} = O_2^+(\mathbb{R})$　　[2 次の回転群]

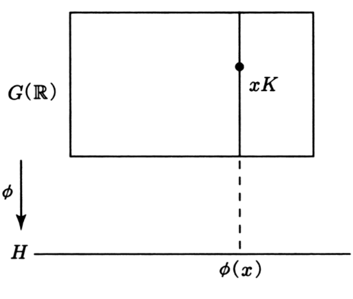
で与えられ

(24)　　$G(\mathbb{R})/K \approx H$

なる全単射が得られます．実際は $G(\mathbb{R})/\{\pm 1\}$ が H に効果的に作用します．そこで，D として上図のように標準的基本領域をとり，ϕ を $x \longmapsto xi, x \in G(\mathbb{R})$, で定まる写像とすると，(16) に登場する F として $\{\pm 1\} \backslash \phi^{-1}(D)$ の基本領域をとることができます．式で書けば

(25)　　$\phi^{-1}(D) = F \cup (-1)F$

という関係になっています．



不変微分形式については，K は単位円ですから

$$\omega_K = dt_1/2t_2$$

を，H では双曲幾何の計量

$$ds^2 = (dx^2 + dy^2)/y^2$$

の定める体積要素

(26) $$\omega_H = \frac{dx \wedge dy}{y^2}$$

をとることができて，運よく

(27) $$\omega_G = \frac{dt_1 \wedge dt_2 \wedge dt_3}{t_1} = \phi^* \omega_H \wedge \omega_K$$

と辻褄があっています．したがって上図の写像 ϕ に関するフビニの公式

(28) $$\int_{G(\mathbf{R})} f(x) \omega_G = \int_H \omega_H \int_K f(xK) \omega_K$$

で $f = \chi_F$, F の特性関数，として (25) に注意すると

(29) $$\int_F \omega_\infty = \frac{1}{2} \int_D \omega_H \int_K \omega_K = \frac{\pi}{2} \int_D \omega_H$$

となり，D の面積の計算に帰します．すなわち

(30) $$\int_D \omega_H = \int_D \frac{dx \wedge dy}{y^2} = \int_{-\frac{1}{2}}^{\frac{1}{2}} dx \int_{\sqrt{1-x^2}}^{\infty} \frac{dx}{y^2} = 2\Big[\sin^{-1} x\Big]_0^{\frac{1}{2}} = \frac{\pi}{3}.$$

(29), (30) から $\displaystyle\int_F \omega_\infty = \frac{\pi^2}{6}$. これと (21), (17) から

(31) $$\tau(G) = 1$$

を得ます．すなわち，この　玉河数 = 1　という‘アデール幾何’の定理の証明の鍵はこのエッセイで素数が無限にあることの証明に使った等式 (4) であったわけです．

●後注……………………

1）砂田利一，連分数のはなし，『数学セミナー』90 年 8 月号，pp. 56-59 は「初整，第 2 章」を明快に要約したすぐれた記事です．

2）$m = 1$ とすれば，ユークリッドの場合になります．

3）$x \geqq 2$ (すなわち $z \equiv 1 \pmod 4$) のとき 1 つ y をきめると z が素数となる x は有限個しかないというのは本当でしょうか？

4）π については「辞典，p. 72」参照．また『数学セミナー』89 年 3 月号に特集・π がありました．

5）「辞典，p. 253」参照．

6）「辞典，p. 2」参照．

7）$\tau(G)$ は，G の $\mathbf{Q}$ で定義された左不変な微分形式のとり方にはよりません．

8）ω_v は ω が $G(\mathbf{Q}_v)$ に定めるハール測度です．

付録 2
方程式を解くことについて

●第 1 日目

§0．はじめに

タイトルは「方程式を解くことについて」となっていますが，「方程式」と申しましても，代数方程式，微分方程式，積分方程式，関数方程式など，いろいろあります．今回は，まずある問題を設定し，その問題を解くために，どういうテクニックが必要であるか，どういう方程式が必要であるかということをやります．難しそうに見える問題なんですが，結論から言いますと，1 次方程式だけで片がつくんです[1)]．

1 次方程式というのは，

$$ax = b$$

という形をしていて，a, b はわかっているが x がわからない．x を a, b でどう表わすかというものです．「わかっているもの」と「わからないもの」があって，「わからないもの」は「わかっているもの」でどういうふうに書けるか．数学を離れてもこういう問題はたくさんあります．たとえばクロスワード・パ

1） 問題の完全な解決には 2 次方程式がいります．この講演では 1 次方程式だけですむ部分的解決に集中したのです．

ズルも方程式の１つといえます．少し簡単な例をやってみましょう．

キ	カ
	ズ

空欄にどういう文字を入れるか．タテ・ヨコが意味を成さなくてはなりません．たとえば「ミ」を入れてみますと，「君，数，幾何，水」となりますから，「ミ」は答えになります．しかし，このパズルを満足する答えは他にもあります．「ス」を入れてみましょう．「キス(魚の名前)，数，幾何，鈴」となります．つまり答は一意的には求まらない，ということです．

もう少し複雑な問題をやってみましょう．今度は枠の中に言葉を入れる問題です．人の名前です．

さあ，空欄に誰を入れるか，考えてみてください．

→ ↓

ユークリッド	ニュートン
デカルト	

答えは，それぞれの人が書いた本を考えればいいのです．ユークリッド『原論』，ニュートン『プリンキピア』，デカルト『方法序説』[2)]ですね．『原論』は幾何学，『プリンキピア』は力学を内容としていますが，ご承知のように『プリンキピア』は『原論』のスタイルを真似て書かれています．ですから，マス

2）『方法叙説』と書くこともあることを森田茂之君が教えてくださいました．この方が《Discours de la méthode》の訳として原稿に忠実でしょうが，ここでは『数学辞典』(岩波，第２版，p.125)に従いました．

の → 方向は，本のスタイルが同じであることを表わしていると言えます．そして ↓ 方向は，代数化あるいは解析化，すなわち式で書いて計算しやすいようにしています．ユークリッドの幾何学に座標を導入し，式で書いて代数化(解析化)したものが，デカルト『方法序説』における解析幾何なんですね．

さて，右下の空欄には誰が入るか，誰が『プリンキピア』を代数化したか．もうおわかりですね．オイラーです．そして著作は『解析力学』ですね．パズルを仕上げてみましょう．

→ スタイル

↓ 代数化(解析化)

ユークリッド 『原論』 (幾何)	**ニュートン** 『プリンキピア』 (力学)
デカルト 『方法序説』 (解析幾何)	**オイラー** 『解析力学』 (解析力学)

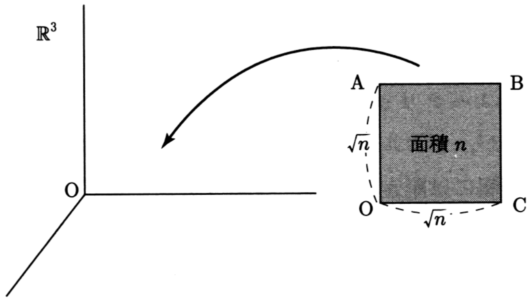
お話はこれくらいにして，本題に入りましょう．

§1．問題

まず問題を呈示しましょう．例によって $\mathbb{R}$ で実数全体，$\mathbb{Z}$ で整数全体を表わします．そして，3次元ユークリッド空間 $\mathbb{R}^3$ を考えます．また，面積 n の正方形 OABC を考えます．n は自然数とします．

さて問題です．正方形の4つの頂点がそれぞれ空間格子点，すなわち $\mathbb{Z}^3$ にのるようにしたいのです．ただし，正方形の頂点 O は $\mathbb{R}^3$ の原点 O にいくようにします．

たとえば $n = 7$ をとるとわかるように，このようなことはいつもできると



は限りません[3]．どのような n についてできるか，あるいは，できないか，という問題です．

念のためくりかえすと次のようになります．

> **問題**　OABC を面積 $n\,(n = 1, 2, \cdots)$ の正方形とするとき，
>
> $O = (0, 0, 0),$
>
> $A, B, C \in \mathbb{Z}^3$　　(空間格子点全体)
>
> とすることは，どのような n について可能であるか？

この講演では 1 次方程式だけで片付く，次の部分解の証明に集中することにします．

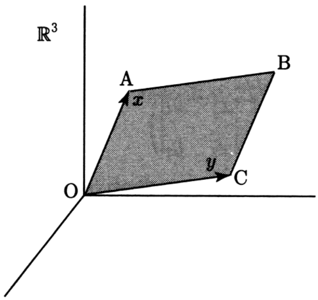
部分解：もしも n が奇数の平方因子を含まないならば，この問題はたかだか座標面でのみ可能である．

つまり，n が奇数の平方因子を含まないならば，面積 n の正方形を座標面以外の空間格子点にのせることはできないのです．(次ページ図)

座標面上だったら，できることもあるし，できないこともある，ということです．

$n = 1, 2, 3, 4, 5, 6, 7, 8$ は奇の平方因子を含まないから同様です．奇の平方因子を含む場合，たとえば $n = 9 = 3^2$ の場合はどうでしょうか．

3)　これは 7 が 3 つの整数の平方の和には書けないことによります．



$$\overrightarrow{\mathrm{OA}} = x = (-1, 2, 2), \qquad \overrightarrow{\mathrm{OB}} = y = (2, -1, 2)$$

とすれば

$$x \perp y, \qquad \|x\|^2 = \|y\|^2 = 9 = n$$

となり，x, y のどの座標も 0 ではないから，空中に吊られた状態になっています．

これは，面積単位で切り売りされている壁紙やプレートをはめ込んでゆくような，室内装飾の問題として応用できるかもしれませんね．ファッショナブルな建物ですと空間格子も使うでしょうしね．

さて，この問題を解いていくわけですが，実はこれは，1 次方程式を体や環($\mathbb{Z} \bmod m$ など)の上で解くことに帰着されます．体の場合は線形代数の問題です．線形代数の目的は 1 次方程式を体上で解くことですから．

ところが，我々の問題では n が自然数ですから，線形代数だけでは解けません．整数論が要ります．つまり合同式

$$ax \equiv b \pmod{m}$$

というのを心得ていなければなりません．ですから，先ほどの問題をアタックするために，今日は，線形代数と初等整数論の常識の復習をやっておきましょう[4)]．

ちょっとその前に，皆さんはベクトル $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$ の内積

$$\langle x, y \rangle = x_1y_1 + x_2y_2 + x_3y_3$$

4）　線形代数の方は少し必要以上のおしゃべりをしますが．

はご存知でしょうが，3 次元という空間に特殊なものとしてベクトル積があります．定義は，

$$x \times y = \left(\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}, \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}, \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \right)$$

です．これが意外に役に立つのです．単に代数的なところだけでなく，整数論の中でも役に立ちます．

その例はガウスの《Disquisitiones arithmeticae(整数論研究)》にもあります．大部分は 2 元 2 次形式ですが，3 元 2 次形式を利用しているところがあり，そこでベクトル積を使っています．ただし $x \times y$ の記号は使われていません．いつも 3 つの座標を全部書いています．そこにベクトル積が使われているとは，ちょっと見ただけではわからない，そういう書き方です．

このベクトル積も，我々の問題を解くのに必要になります．

さて，我々の問題の多次元化はすぐ考えられます．たとえば 4 次元空間に，与えられた面積 n の正方形をはめ込むことができるか，という問題になりますが，これから使う方法そのままではできません．ベクトル積は 3 次元でしか使えないからです．

では，復習をはじめましょう．

---

§2．体

$$ax = b, \qquad a, b \in \mathbb{R}$$

を解くと，

$$a \neq 0 \quad \text{ならば} \quad x = \frac{b}{a},$$

$$a = 0 \quad \text{ならば} \quad \begin{cases} x \text{ はない} & (b \neq 0) \\ x \text{ は何でもよい} & (b = 0) \end{cases}$$

となります．ここで，a, b を実数としましたが，四則演算ができるということ

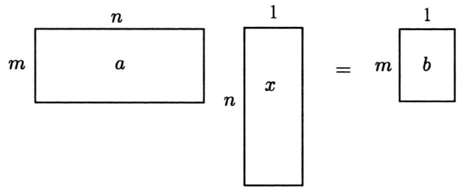
しか使っていませんから，実数である必要はありません．つまり

$$a, b \in K \quad (体)$$

で十分です．これで体の復習はおしまいです．

§3．線形代数

$a=(a_{ij})\,(a_{ij} \in K)$ を (m, n) 行列とします．$ax=b$ の意味は，図を描いてみると



となります．成分ごとに書けば連立1次方程式になりますね．

行列は，ベクトルをベクトルに対応させる関数であると考えます．四角いなかに数がつまっているものと考えると本質がわからなくなってしまいます．

さて，n 次元タテ・ベクトル空間 K^n から m 次元タテ・ベクトル空間 K^m への関数 $f(x)=ax$ を考えます．

$$K^n \xrightarrow{f} K^m$$

f は線形性をもちます．つまり α, β をスカラーとするとき $(\alpha, \beta \in K)$,

$$f(\alpha x+\beta y)=\alpha f(x)+\beta f(y)$$

が成り立ちます．

この関数を調べてみましょう．f は線形ですから核(kernel)と像(image)が大切です．

核：　$\mathrm{Ker}\, f=\{x \in K^n\,;\, f(x)=0\}$

$$像：\quad \mathrm{Im}\, f = \{ f(x) \in K^m\, ; x \in K^n \}$$

f の線形性によって，Ker f は K^n の部分空間，Im f は K^m の部分空間となります．それぞれの次元について次の大切な関係があります．

$$\dim(\mathrm{Ker}\, f) + \dim(\mathrm{Im}\, f) = n.$$

ここで

$$\dim(\mathrm{Im}\, f) = a \text{ の rank}$$
$$= a \text{ の 1 次独立なタテ・ベクトルの数}$$

です．核の次元というのは，同次方程式 $ax = 0$ の解空間がどれくらい大きいかを測るものですが，上の関係は a の rank と解空間の次元とは相対的になっていて，一方が大きければ他方が小さくなるということを意味します．つまり，独立な解の数は，a の rank を計算して，それを n から引けばよい，ということです．

これで同次(homogneous)の場合の話はお終いです．我々が本当に解きたいのは $ax = b$ の非同次の場合(つまり $b \neq 0$)です．それを次にやりましょう．

$$a, b \in K^m, \qquad f(x) = ax$$
$$解空間：\quad S = \{ x \in K^n\, ; f(x) = b \}$$

とします．$S \neq \phi$ の場合を考えましょう．

$$S \neq \phi \iff b \in \mathrm{Im}\, f \iff \mathrm{rank}\, a = \mathrm{rank}(a, b)$$
$$(= r \text{ とします})$$

です．

さて，$f(x) = b$ は同次ではないから，微分方程式でやるように 1 つ特殊解を見つけ，それを x_0 とします．x を勝手な解としますと，

$$f(x) - f(x_0) = b - b = 0.$$

左辺は f の線形性により，$f(x - x_0)$ となりますから，

$$x - x_0 \in \mathrm{Ker}\, f$$

となります．すなわち，1 つ特殊解が見つかりさえすれば，解空間 S は次のように書けます．

$$S = x_0 + \mathrm{Ker}\, f.$$

S の次元は Ker f と同じ，つまり $n - r$ ですね．

まとめてみますと

$$S = \begin{cases} \phi & (b \notin \mathrm{Im}\, f), \\ x_0 + \mathrm{Ker}\, f & (b \in \mathrm{Im}\, f). \end{cases}$$

これは第2節で述べた，$a, b \in K$ の場合の，行列への拡張になっています．

§4．初等整数論

ここでは $\mathbb{Z} = \{0, \pm 1, \pm 2, \cdots\}$ が問題になります．これは体ではなく環です．すなわち割り算ができることもあれば，できないこともあります．

整数 $m \geqq 2, a, b \in \mathbb{Z}$ とします．

$$m \mid a-b \qquad (m \text{ が } a-b \text{ を割る})$$

のとき，a と b が m を法として合同であるといい，

$$a \equiv b \quad (m)$$

と書きます．mod m と書くこともあるのですが，ここでは簡単に (m) を使います．m をきめてあるときは単に $a \equiv b$ とも書きます．

同値関係

$$\begin{cases} a \equiv a \\ a \equiv b \iff b \equiv a \\ a \equiv b, b \equiv c \implies a \equiv c \end{cases}$$

が成り立つので，この関係によって整数全体を類に分けることができます．つまり，m で割っていくつ余るかによって分類するのです．そして，その類を点と考えた集合ができます．これを

$$\mathbb{Z}/m\mathbb{Z}$$

と書きます．各類の代表として，$0, 1, \cdots, m-1$ がとれますから，この集合は m の個の点から成ります．$\mathbb{Z}/m\mathbb{Z}$ は足し算，掛け算ができますから環になります．これは体になることもありますが，そのための必要十分条件は「m が素数である」ことです．

実例をやってみましょう．

例 1　$x^2 \equiv x \quad (2)$.

証　$x^2 - x = x(x-1) \equiv 0 \quad (2)$.

例 2　$x^2 \equiv 0$ または $1 \quad (4)$.

証　x が偶数の場合は　$x^2 \equiv 0 \quad (4)$.
奇数の場合は $x = 2y+1$ とおくと，$x^2 = 4y^2+4y+1 \equiv 1 \quad (4)$.

例 3　$\mathbb{Z}/2\mathbb{Z}$ は，代表元として 0 と 1 がとれますが，これだけでちゃんと体になります．＋，× の表が作れます．

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

逆元の存在も明らかです．

ここで，初等整数論はこれしかないというくらい，重要でやさしい定理を 3 つばかりやりましょう[5)]．

定理 4.1　$x_1, \cdots, x_n \in \mathbb{Z}$ をとり (ただし $(x_1, \cdots, x_n) \neq (0, \cdots, 0)$)，

$$M = \{\lambda_1 x_1 + \cdots + \lambda_n x_n\,;\, \lambda_i \in \mathbb{Z}\}$$

とすると，

$$M = d\mathbb{Z}$$

ただし $d = (x_1, \cdots, x_n) = x_1, \cdots, x_n$ の最大公約数

となる．

ここで集合を M としたのは module(加群) のつもりです．加群とは ＋，－ について閉じているものです．また $(x_1, \cdots, x_n)$ は $x_1, \cdots, x_n$ の最大公約数を表わしますが，ベクトルと紛らわしいので注意してください．

5）任意の自然数が一意的に素因子分解できるという，いわゆる整数論の基本定理はもちろん基本的ですが，ここでは証明なしに使うことにしました．ただし，定理 4.1 はこの基本定理の証明にも役立ちます．

証明　$x_1, \cdots, x_n$ には少なくとも1つ0でないものがあります．その係数を1とし，他の係数を0とすれば，その数自身が M に入りますから，0でない元が M に入ります．そしてその符号を替えたものも入りますから，M は少なくとも1つ正の整数を含みます．その中で最小のものを d とすればいいのです．くわしくやってみましょう．

d を M の中の最小正整数とします．$M \supseteqq d\mathbb{Z}$ は明らかですから $M \subseteqq d\mathbb{Z}$ を示しましょう．$x \in M$ を任意にとり，$x \in d\mathbb{Z}$ を示せばいいのです．d で割ってみましょう．

$$x = qd + r, \qquad 0 \leqq r \leqq d-1.$$

$r = 0$ ならば $x \in d\mathbb{Z}$ となります．$r \neq 0$ ならば

$$r = x - qd \in M$$

となり，d の最小性に矛盾してしまいます．

次に d が最大公約数であることを示します．

$$d = (x_1, \cdots, x_n) \iff \begin{array}{ll} (1) & d \mid x_1, \cdots\cdots, d \mid x_n \\ (2) & t \mid x_1, \cdots\cdots, t \mid x_n \implies t \mid d \end{array}$$

ですから，上の (1)，(2) に分けてやってみましょう．

(1)　$x_i\,(i = 1, \cdots, n)$ は M の元ですから，$M = d\mathbb{Z}$ より $x_i = dx_i'$ と書けます．すなわち $d \mid x_i\,(i = 1, \cdots, n)$．

(2)　d も M の元ですから

$$d = \lambda_1 x_1 + \cdots + \lambda_n x_n$$

と書けます．また $x_i = tx_i'$ ですから，

$$d = \lambda_1 t x_1' + \cdots + \lambda_n t x_n' = t(\lambda_1 x_1' + \cdots + \lambda_n x_n').$$

したがって $t \mid d$ となります．　　　　　　　　　　　　　　　　　　　　(証終)

系1　$x = (x_1, x_2, x_3) \in \mathbb{Z}^3\,(x \neq 0)$，$d = (x_1, x_2, x_3)$ とすると，ある $y \in \mathbb{Z}^3$ で，$\langle x, y \rangle = d$ とできる．

証明　y として $(\lambda_1, \lambda_2, \lambda_3)$ ととればいいですね．

系2　$d = (x_1, x_2, x_3) = 1$ のとき，ある $y \in \mathbb{Z}^3$ で，$\langle x, y \rangle = 1$ とできる．

今後，$(x_1, x_2, x_3) = 1$ のとき，x を原始ベクトルとよびます．

定理 4.2　$a, b \in \mathbb{Z}$,　$(a, m) = 1$ ならば

$$ax \equiv b \quad (m)$$

は m を法として一意的に解ける．

証明　i)　一意性．

$$ax \equiv b \quad (m), \qquad ax' \equiv b \quad (m)$$

としますと，

$$ax - ax' = a(x - x') \equiv 0 \quad (m).$$

$(a, m) = 1$ ですから $x \equiv x'\ (m)$ となります．

ii)　存在．上の系 2 より，$ax' + my' = 1$ を満足する (x', y') があります．両辺に b を掛けて

$$ax'b + my'b = b.$$

これより

$$ax'b \equiv b \quad (m)$$

となり，ここで $x'b$ を改めて x とすればいいですね．　　　　　　　　　　　　　　(証終)

定理 4.3　$a_1, \cdots, a_l \in \mathbb{Z}$ が与えられ，m の 1 つの分解を

$$m = m_1 \cdots m_l \qquad \text{ただし} \quad (m_i, m_j) = 1 \quad (i \neq j)$$

とするとき，連立方程式

$$\begin{cases} x \equiv a_1 \quad (m_1) \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv a_l \quad (m_l) \end{cases}$$

を満足する解 x が m を法として一意的にきまる．

証明　一意性は明らかですから，存在を示します．m を m_i と残りの部分に分けます．つまり

$$m = m_1 \cdots m_l = m_i \cdot m_i^*$$

とします．明らかに

$$(m_i, m_i^*) = 1, \qquad m_j \mid m_i^* \qquad (j \neq i)$$

ですね．先ほどの定理 4.2 より，

$$m_i^* x_i \equiv 1 \quad (m_i)$$

は一意的に解けます．そこで

$$x = a_1 m_1^* x_1 + \cdots\cdots + a_l m_l^* x_l$$

とおけばいいのです．

$$x \equiv a_i m_i{}^* x_i \quad (m_i)$$
$$\equiv a_i \quad (m_i)$$

となりますでしょう．q.e.d.

この q.e.d. は本当は quod erat demonstrandum（これが証明すべきことであった）なんですが，アメリカの数学者 H. M. Stark は quite easily done の略だと言っています[6)]．今の証明はまさに quite easily done ですね．

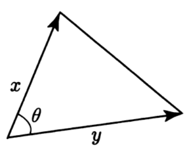
さて，次にベクトル解析の復習をしておきましょう．

§5．$\mathbb{R}^3$ での内積とベクトル積

内積

$$\langle x, y\rangle = x_1y_1 + x_2y_2 + x_3y_3$$

は双線形です．つまり，x を固定すれば y について線形，y を固定すれば x について線形になります．また対称的，すなわち x, y を入れ替えても同じです．幾何学的には，角度を測るともいえます．



としますと，

$$\cos\theta = \frac{\langle x, y\rangle}{\|x\|\,\|y\|},$$

$$\text{ただし } \|x\| = \sqrt{Nx},\ Nx = x_1{}^2 + x_2{}^2 + x_3{}^2 = \langle x, x\rangle$$

6）　H. M. Stark, An Introduction to Number Theory, The MIT Press, 1978 の 224 ページの脚注参照．

となります．Nx をノルムとよびます．内積とノルムには次の関係があります．

$$2\langle x, y\rangle = N(x+y)-Nx-Ny.$$

ベクトル積 $x\times y$ は，x, y を入れかえると符号が変わります．また，ベクトル積の性質には，通常の線形性に加えて次のようなものがあります．

i） $y\times x = -(x\times y)$

ii） $\langle x, y\times z\rangle = |x, y, z|$ （行列式）

iii） $x\times(y\times z) = \langle x, z\rangle y-\langle x, y\rangle z$

iv） $\langle x\times y, u\times v\rangle = \langle x, u\rangle\langle y, v\rangle-\langle x, v\rangle\langle y, u\rangle$

iii）と iv）は宿題としましょう．正直に忍耐強く計算すると出てきます．iv）で $u = x, v = y$ とすると

$$N(x\times y) = Nx\cdot Ny-\langle x, y\rangle^2$$

となり，これはよく知られている，コーシー‐ラグランジュの公式です．

幾何学的にはベクトル積は次のような意味があります．

$x \neq 0, y \neq 0$ のとき，

$$x\times y = 0 \iff x /\!\!/ y \iff y = ax \qquad (a \in \mathbb{R})$$

さて，今日復習してきたことがらを使って，証明したい定理があります．

定理 5.1 $x = (x_1, x_2, x_3) \in \mathbb{Z}^3$, $y = (y_1, y_2, y_3) \in \mathbb{Z}^3$，$x$ は原始ベクトル，つまり $(x_1, x_2, x_3) = 1$ とします．このとき，

$$x\times y \equiv 0 \quad (m)$$

ならば，ある $a \in \mathbb{Z}$ によって

$$y \equiv ax \quad (m)$$

とできる．

今日やったことは，どれもみなやさしいことばかりです．それらをうまく組み合わせると，この定理が証明できるわけです．この定理を使って，今日はじめに掲げた問題を解くことができます．証明を考えてごらんなさい．

今日はここで終りにしましょう．

［1985 年 5 月 14 日，立教大学にて］

●第2日目

§6．定理5.1の証明

前回，最後に紹介しました定理の証明からはじめましょう．

定理5.1　$x=(x_1, x_2, x_3) \in \mathbb{Z}^3, y=(y_1, y_2, y_3) \in \mathbb{Z}^3, x$ は原始ベクトル，つまり $(x_1, x_2, x_3)=1$ とします．このとき，

$$x \times y \equiv 0 \quad (m)$$

ならば，ある $a \in \mathbb{Z}$ によって

$$y \equiv ax \quad (m)$$

とできる．

証明　m の素因子分解

$$m=\prod p_i^{\alpha_i}$$

を考えます．まず，1つの $p=p_i$ に注目し，法 p^α について考え，最後にまとめて m の場合を考えます．

$(x_1, x_2, x_3)=1$ ですから $x_i\,(i=1,2,3)$ のうち少なくとも1つは p と素です．たとえば x_3 が p と素であるとしてみましょう．すると

$$(p^\alpha, x_3)=1$$

となりますね．前回証明しました定理4.2により，ある $\lambda, \mu \in \mathbb{Z}$ により

$$\begin{cases} x_3\lambda \equiv x_1 \quad (p^\alpha) & (1) \\ x_3\mu \equiv x_2 \quad (p^\alpha) & (2) \end{cases}$$

とすることができます．

条件

$$x \times y = \left(\begin{vmatrix} x_2 & y_2 \\ x_3 & y_3 \end{vmatrix}, \begin{vmatrix} x_3 & y_3 \\ x_1 & y_1 \end{vmatrix}, \begin{vmatrix} x_1 & y_1 \\ x_2 & y_2 \end{vmatrix} \right) \equiv (0, 0, 0) \quad (p^\alpha)$$

の各座標をみますと，次のようになります．

$$x_2y_3 \equiv x_3y_2 \quad (p^\alpha), \qquad (3)$$

$$x_3y_1 \equiv x_1y_3 \quad (p^\alpha). \tag{4}$$

(3)の左辺に(2)を代入すると

$$y_3x_3\mu \equiv x_3y_2 \quad (p^\alpha.)$$

$(p^\alpha, x_3) = 1$ ですから，x_3 を消去できます．すなわち

$$y_2 \equiv \mu y_3 \quad (p^\alpha).$$

同様にして，(4) に (1) を代入し，x_3 を消去すると，

$$y_1 \equiv \lambda y_3 \quad (p^\alpha)$$

となります．したがって，ベクトル y は

$$y = (y_1, y_2, y_3) \equiv (\lambda y_3, \mu y_3, y_3) = y_3(\lambda, \mu, 1) \quad (p^\alpha) \tag{5}$$

と書けます．

一方，$(p^\alpha, x_3) = 1$ と定理 4.2 より，

$$x_3x \equiv 1 \quad (p^\alpha)$$

は一意的に解けますから，その解を $x_3{}^*$ とします．つまり

$$x_3x_3{}^* \equiv 1 \quad (p^\alpha)$$

とします．

(1) の両辺にこの解 $x_3{}^*$ を掛けてみますと

$$x_3x_3{}^*\lambda \equiv x_1x_3{}^* \quad (p^\alpha),$$

すなわち

$$\lambda \equiv x_1x_3{}^* \quad (p^\alpha) \tag{6}$$

となります．同様に (2) の両辺に $x_3{}^*$ を掛けて

$$\mu \equiv x_2x_3{}^* \quad (p^\alpha). \tag{7}$$

(5) に (6), (7) を代入すると

$$\begin{aligned} y &\equiv y_3(\lambda, \mu, 1) \equiv y_3(x_1x_3{}^*, x_2x_3{}^*, x_3x_3{}^*) \equiv y_3x_3{}^*(x_1, x_2, x_3) \\ &\equiv y_3x_3{}^*x \quad (p^\alpha) \end{aligned}$$

となりますが，$y_3x_3{}^* \in \mathbb{Z}, p = p_i$ でしたから $y_3x_3{}^* = a_i$ とおいて，

$$y \equiv a_ix \quad (p_i{}^\alpha).$$

今度は定理 4.3 を使います．

$$\begin{cases} x \equiv a_1 \quad (p_1{}^{\alpha_1}) \\ \cdots\cdots\cdots\cdots\cdots \\ x \equiv a_l \quad (p_l{}^{\alpha_l}) \end{cases}$$

は，m を法として一意的に解けますから，その解を a とします．

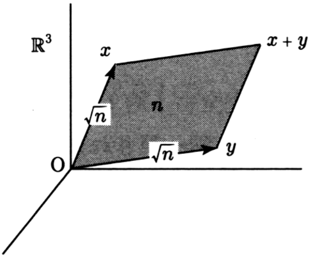
$$y \equiv a_i x \equiv ax \quad (p_i^{\alpha_i}).$$

これがすべての $i\,(i=1,\cdots,l)$ について成り立つわけですから，$p_i^{\alpha_i}$ をすべて掛け合わせたもの，つまり法 m について成り立ちます．q.e.d.

3 次元のベクトル空間と，初等整数論を組み合わせて証明できたわけです．難しくないでしょう．定理を見ていてもユークリッド空間との類似から直観的に成立しそうな気がしますね．直観的に成り立ちそうなことは，証明しようと思えばたいていできます[7]．「こういうことが成り立つであろう」と思うことの方が証明より大切です．

§7．$M(n) \rightleftarrows V(n)$

さて，いよいよ問題の攻略にかかります．問題をもう一度申しますと，紙で面積が n である正方形をつくり，その 4 頂点が $\mathbb{R}^3$ の格子点に(ただし 1 つの頂点は $\mathbb{R}^3$ の原点に)載るようにしよう，というものです．



つまり次のようになります．

7）　これが“直観”というものの特性です．

問題　OABC を面積 $n\,(n=1,2,\cdots)$ の正方形とするとき，

$$\mathrm{O}=(0,0,0),$$

$$\mathrm{A},\mathrm{B},\mathrm{C}\in\mathbb{Z}^3 \qquad \text{(空間格子点全体)}$$

とすることは，どのような n について可能か？

これが n によって，できたりできなかったりする例は前回やりました．

さて，攻略の方針です．ある集合を設定しますが，その集合だけを見ていても何もわかりませんから，もっとわかりやすそうな集合におきかえます．おきかえた後に，それを細かくきざんで考えます．

さて，はじめましょう．与えられた n に対して，上に述べた正方形にあたる集合を式に書いてみましょう．

$$V(n)\overset{\mathrm{def}}{=}\{(x,y)\in\mathbb{Z}^3\times\mathbb{Z}^3\,;Nx=n,Ny=n,\langle x,y\rangle=0\}.$$

ただし，$Nx=\|x\|^2={x_1}^2+{x_2}^2+{x_3}^2$.

というベクトルの対の全体を考えます[8]．つまり，$V(n)$ がいつ空集合になるか，あるいはならないか，という問題になります．

ちょっと天降り的ですが，次のような集合 $M(n)$ を考えるとうまくいくんです．

$$M(n)\overset{\mathrm{def}}{=}\{(x,v)\in\mathbb{Z}^3\times\mathbb{Q}^3\,;Nx=n,Nv=1,\ \langle x,v\rangle=0,x\times v\in\mathbb{Z}^3\}.$$ [9]

$V(n)$ と $M(n)$ は集合として完全に 1 対 1 の対応がついています．言いかえると，ある φ という写像によって同一視されます．すなわち，

(#)　　$M(n)\xrightarrow[\sim]{\varphi}V(n)$

具体的には

$$\varphi(x,v)=(x,x\times v)$$

とすればいいのです．(#) を示すためには，次の 3 つのことを言わなくてはな

8）　ベクトルの対 (x,y) を枠 (frame) ともいいます．

9）　$\mathbb{Q}$ は有理数体をあらわします．

りません．

①　φ は well-defined である．

②　φ は1対1写像である．

③　φ は上への(onto)写像である．

証明　①　$\varphi(x, v) = (x, x\times v)$ が $V(n)$ に入っていればいいのですから，$x \times v = y$ とおいて1つ1つチェックしてみましょう．

$(x, y) \in \mathbb{Z}^3\times\mathbb{Z}^3$ は $y = x\times v \in \mathbb{Z}^3$ ですから明らか．

$$\begin{aligned} Ny &= N(x\times v) = Nx\cdot Nv - \langle x, v\rangle^2 \\ &\qquad\text{(コーシー－ラグランジュの公式)} \\ &= Nx\cdot 1 - 0^2 = Nx = n. \end{aligned}$$

$$\langle x, y\rangle = \langle x, x\times v\rangle = |x, x, v| = 0.$$

したがって φ は well-defined です．

②　1対1ということは，ちがうものはちがうところにいくということです．すなわち

$$\varphi(x, v) = \varphi(x', v') \implies (x, v) = (x', v')$$

をいえばいいのです．仮定から

$$(x, x\times v) = (x', x'\times v')$$

で，各座標を比較して

$$x = x', \qquad x\times v = x'\times v' = x\times v'.$$

移項して

$$x\times(v'-v) = 0.$$

$x \neq 0$ だから，x と $v'-v$ は平行，すなわち

$$v'-v = \lambda x.$$

一方，$0 = \langle x, v\rangle = \langle x, v'\rangle$ だから

$$0 = \langle x, v'-v\rangle = \langle x, \lambda x\rangle = \lambda\langle x, x\rangle = \lambda Nx = \lambda n,$$

$$\therefore \quad \lambda = 0.$$

ゆえに $v = v'$．

③　φ が上への写像であることを言うためには，$(x, y) \in V(n)$ を勝手にとったとき，$v \in \mathbb{Q}^3$ を，$(x, v) \in M(n)$ かつ $x\times v = y$ となるようにとれればいいわけです．

このために

$$v = \frac{1}{n}(y \times x) \in \mathbb{Q}^3$$

とおくとよいことが次のようにしてわかります．まず

$$x \times v = \frac{1}{n}(x \times (y \times x)) = \frac{1}{n}(\langle x, x\rangle y - \langle x, y\rangle x)$$

$$= \frac{1}{n} Nx \cdot y = y$$

で，$x \times v = y \in \mathbb{Z}^3$ はよろしい．

次に $(x, v) \in M(n)$ をいうのですが，$Nx = n$ は同語反復です．また

$$\langle x, v\rangle = \langle x, \frac{1}{n}(y \times x)\rangle = \frac{1}{n}\langle x, y \times x\rangle = \frac{1}{n}|x, y, x| = 0$$

で $\langle x, v\rangle = 0$ もよろしい．

最後に

$$Nv = \frac{1}{n^2}N(y \times x) = \frac{1}{n^2}(Ny \cdot Nx - \langle y, x\rangle^2)$$

$$= \frac{1}{n^2}(n \cdot n - 0^2) = \frac{1}{n^2} \cdot n^2 = 1,$$

すなわち $Nv = 1$ もよろしい[10)]．

以上により，$V(n)$ と $M(n)$ とは同一視できました．つまり「$V(n)$ がいつ空集合になるか」という問題は，「$M(n)$ がいつ空集合になるか」という問題と同じです．

---

10) ③の証明は講演のときの私の下手な証明を，佐藤文広君の上手な証明（$v = \frac{1}{n}(y \times x)$ とおくこと）でおきかえたものです．

§8．$M_m(n)$

ここで，$v\,(\neq 0) \in \mathbb{Q}^3$ のオーダーという概念を入れましょう．何倍したら分母を払うことができるか，という最小の数です．正確に言うと，$\mu v \in \mathbb{Z}^3$ となる自然数 μ の中で最小の数を v のオーダーといい，ord v で表わします．たとえば $v = \left(\frac{6}{7}, \frac{8}{7}, \frac{10}{7}\right)$ のときは ord $v = 7$ ですね．

このオーダーごとに $M(n)$ を切りきざんでみましょう．$m \geqq 1$ をとり

$$M_m(n) \overset{\text{def}}{=} \{ (x, v) \in M(n) ; \operatorname{ord} v = m \}$$

と定義します．

明らかに

$$M_m(n) \cap M_{m'}(n) = \phi \qquad (m \neq m')$$

ですね．ここで注意したいことは，$V(n)$ は有限集合ですから[11]，$M(n)$ も有限集合である，ということです．

$$M(n) = \bigcup_{n=1}^{\infty} M_m(n) \qquad \text{(disjoint)}$$

と，形式的には無限和の形で書けますが，$M_m(n)$ は有限個の m を除いて空でなければいけません．

補題を1つやりましょう．

補題 8.1　$v \in \mathbb{Q}^3, Nv = 1, \operatorname{ord} v = m$ ならば，$mv \in \mathbb{Z}^3$ で，mv は原始ベクトルである．

証明　$mv = du$ ($u \in \mathbb{Z}^3$ は原始ベクトル) とし，$d = 1$ を言えばいいですね．

$$N(mv) = N(du)$$

11)　$(x, y) \in V(n)$ ならば $Nx = x_1{}^2 + x_2{}^2 + x_3{}^2 = n, x_i \in \mathbb{Z}$, より x は有限です．y も同様．

より

$$m^2 Nv = m^2 = d^2 Nu,$$

したがって

$$d^2 \mid m^2 \qquad \text{すなわち} \qquad d \mid m$$

となります．

一方，$\frac{m}{d}v = u$ において，u が原始ベクトル，$\mathrm{ord}\, v = m$ ですから，$d = 1$ でなければなりません．q.e.d.

先ほどの例 $v = \left(\frac{6}{7}, \frac{8}{7}, \frac{10}{7}\right)$ では，$\mathrm{ord}\, v = 7$ でしたが，$7v = (6, 8, 10)$ は原始ベクトルではありません．

$$Nv = \frac{1}{49}(36+64+100) \neq 1$$

だからです．補題 8.1 で $Nv = 1$ という条件がどうしても必要なのです．

§9．$M_m(n) \xrightarrow{\sim} M_m{}^*(n)$

さて，上のように，$M(n)$ を $M_m(n)$ にきざんだら，もう一度，別な集合におきかえます．

$$M_m{}^*(n) \overset{\mathrm{def}}{=} \{(x, u) \in \mathbb{Z}^3 \times \mathbb{Z}^3 ; Nx = n, u \text{ は原始ベクトル，} Nu = m^2, \langle x, u \rangle = 0, x \times u \equiv 0\,(m)\}$$

と定義します．何が言いたいのかというと，ある ϕ という写像により，$M_m(n)$ と $M_m{}^*(n)$ が集合として完全に 1 対 1 に対応がつく，すなわち

$$(**) \qquad M_m(n) \xrightarrow[\sim]{\phi} M_m{}^*(n)$$

ということです．

$M_m(n)$ をもう一度書いておきましょう．

$$M_m(n) = \{ (x, v) \in \mathbb{Z}^3 \times \mathbb{Q}^3 ; Nx = n, Nv = 1, \langle x, v \rangle = 0, x \times v \in \mathbb{Z}^3, \ \mathrm{ord}\, v = m \}.$$

ψ は

$$\psi(x, v) = (x, mv)$$

とすればいいのです．mv が $M_m{}^*(n)$ の u になります．先ほどやりましたように，次の 3 つのことが言えればいいのです．

① ψ は weell-defined である．

② ψ は 1 対 1 写像である．

③ ψ は上への(onto)写像である．

証明　①　$\psi(x, v) = (x, mv)$ が $M_m{}^*(n)$ の性質を満足するか，1 つ 1 つチェックすればいいのです．

$u = mv$ が原始ベクトルであることは，上の補題 8.1 そのものです．また，

$$Nu = Nmv = m^2 Nv = m^2.$$

残りも明らかですね．

②　ただスカラー倍しただけですから，1 対 1 は明らかです．

③　$u \in M_m{}^*(n)$ を与えて $v = \dfrac{u}{m}$ とおき (x, v) が $M_m(n)$ の性質を満足することを言えばいいのです．

問題は $\mathrm{ord}\, v = m$ であることですね．$mv = u \in \mathbb{Z}^3$ ですから，m はオーダーの候補ではあるわけです．あとは m が最小であること，すなわち $\mu v \in \mathbb{Z}^3$ ならば $m \mid \mu$ であることを言えばいいのです．

$$\mu \cdot \frac{u}{m} = w \in \mathbb{Z}^3 \qquad \text{つまり} \qquad \mu u = mw$$

とします．u は原始ベクトルですから，ある $\lambda \in \mathbb{Z}^3$ により

$$\langle \lambda, u \rangle = 1$$

とできます(定理 4.1 の系 2)．

$$\mu = \langle \lambda, \mu u \rangle = \langle \lambda, mw \rangle = m \langle \lambda, w \rangle$$

で，$\langle \lambda, w \rangle \in \mathbb{Z}$ だから $m \mid \mu$．したがって $\mathrm{ord}\, v = m$．

この部分だけが，non-trivial ですね．q.e.d.

§ 10．$M_m(n) \neq \phi \Longrightarrow m$ は奇数

さて，m が偶数か奇数かによって，わかることがあります．次の (※) が成り立つのです．

(※)　　$M_m(n) \neq \phi \implies m$ は奇数．

逆に言えば，m が偶数ならば $M_m(n) = \phi$ となってしまう，ということです．証明してみましょう．

証明　$M_m(n)$ が空でないならば，(∗∗) により $M_m{}^*(n)$ も空ではありませんから，$M_m{}^*(n)$ から元を１つとりそれを (x, u) としましょう：

$$(x, u) \in M_m{}^*(n).$$

$M_m{}^*(n)$ の元ですから，u は原始ベクトルで

$$Nu = u_1{}^2 + u_2{}^2 + u_3{}^2 = m^2$$

を満たさなければなりません．

m を偶数と仮定し，矛盾を導きましょう．

$$u_1{}^2 + u_2{}^2 + u_3{}^2 \equiv 0 \quad (4)$$

となりますが，こうなる $(u_1{}^2, u_2{}^2, u_3{}^2)$ の組み合わせはごくわずかです．$u_i{}^2 \equiv 0, 1\ (4)$ ですから，候補を全部書いても知れています．

(0,0,0)　(1,0,0)　(0,1,0)　(0,0,1)　(1,1,0)

(1,0,1)　(0,1,1)　(1,1,1)

この中で足して 0 になるものは (0,0,0) だけですが，これは原始ベクトルではありません，結局，全部駄目ですね．すなわち m は偶数ではあり得ない，ということです．q.e.d.

§11. $M_m(n) \neq \phi \Longrightarrow m^2 \mid n_0$

$n = 2^e n_0$, n_0：奇数としますと，もう少し強い結果が成り立ちます．

(※※)　$M_m(n) \neq \phi \quad \Longrightarrow \quad m^2 \mid n_0.$

証明　先ほどと同様に，$M_m(n)$ が空でないならば，$M_m{}^*(n)$ も空ではありませんから，$M_m{}^*(n)$ から元を1つとりそれを (x, u) とします：

$$(x, u) \in M_m{}^*(n).$$

$(x, u) \in \mathbb{Z}^3 \times \mathbb{Z}^3$ の満たす性質を念のために書いてみましょう．

(i)　$Nx = n.$

(ii)　$Nu = m^2.$

(iii)　u は原始ベクトル．

(iv)　$\langle x, u \rangle = 0.$

(v)　$x \times u \equiv 0 \quad (m).$

今日最初に証明しました定理5.1を使うと，(iii), (v)から，ある $a \in \mathbb{Z}$ により

$$x \equiv au \quad (m)$$

とできます．つまり

$$x = au + mv, \qquad v \in \mathbb{Z}^3$$

と書けるわけです．

また，(iv) から

$$0 = \langle x, u \rangle = \langle au + mv, u \rangle = a\langle u, u \rangle + m\langle u, v \rangle$$
$$= aNu + m\langle u, v \rangle = am^2 + m\langle u, v \rangle.$$

したがって

$$\langle u, v \rangle = -am$$

となります．ここで

$$2^e n_0 = n = Nx = \langle au + mv, au + mv \rangle$$
$$= a^2 Nu + 2am\langle u, v \rangle + m^2 Nv$$

$$= a^2Nu - 2a^2m^2 + m^2Nv$$
$$= -a^2m^2 + m^2Nv = m^2(Nv - a^2)$$

m は奇数だから

$$m^2 \mid n_0.$$

つまり§7の(#)と合わせて次のことが証明できました.

定理 11.1 $V(n) \approx M(n) = \bigcup_{m^2 \mid n_0} M_m(n).$

ただし $n = 2^e n_0$, n_0 は奇数.

系 もし n_0 が1以外の平方因子を含まなければ

$$V(n) \approx M_1(n).$$

---

§12. 部分解の証明

今度は $M_1(n)$ の構造を調べてみましょう.

$$M_1(n) = \{ (x, v) \in \mathbb{Z}^3 \times \mathbb{Q}^3 \,;\, Nx = n, Nv = 1, \langle x, v \rangle = 0, x \times v \in \mathbb{Z}^3, \operatorname{ord} v = 1 \}$$

$\operatorname{ord} v = 1$ ということは, $v \in \mathbb{Z}^3$ と同じことですね. $v \in \mathbb{Z}^3$ で長さが1ですから全部を数えあげることができます. 可能な $v = (v_1, v_2, v_3)$ の組は

$$(\pm 1, 0, 0), \qquad (0, \pm 1, 0), \qquad (0, 0, \pm 1)$$

のみです. 一方, $\langle x, v \rangle = 0$ ですから, それぞれに対応して x は

$$(0, x_2, x_3), \qquad (x_1, 0, x_3), \qquad (x_1, x_2, 0)$$

という形になります.

ここで, $\varphi : M_1(n) \xrightarrow{\sim} V(n)$ の φ は具体的には $\varphi(x, v) = (x, x \times v)$ でしたから, $(x, x \times v) \in V(n)$ を全部ひろいあげてみましょう.

いま, たとえば $v = (\pm 1, 0, 0)$ としてみます. このとき $x \times v$ は

$$x \times v = \left(\begin{vmatrix} x_2 & v_2 \\ x_3 & v_3 \end{vmatrix}, \begin{vmatrix} x_3 & v_3 \\ x_1 & v_1 \end{vmatrix}, \begin{vmatrix} x_1 & v_1 \\ x_2 & v_2 \end{vmatrix} \right) = (0, \pm x_3, \mp x_2)$$

となります．同様にして

$$v = (0, \pm 1, 0) \quad \text{のとき} \quad x \times v = (\mp x_3, 0, \pm x_1),$$

$$v = (0, 0, \pm 1) \quad \text{のとき} \quad x \times v = (\pm x_2, \mp x_1, 0)$$

となります．これから $V(n)$ を次のように書くことができます．

（☆）　　$n = 2^e n_0$:　n_0 が平方因子を含まない

とすると，

$$\begin{aligned} V(n) = &\{ (0, x_2, x_3), (0, \pm x_3, \mp x_2) ; {x_2}^2 + {x_3}^2 = n \} \\ &\cup \{ (x_1, 0, x_3), (\mp x_3, 0, \pm x_1) ; {x_1}^2 + {x_3}^2 = n \} \\ &\cup \{ (x_1, x_2, 0), (\pm x_2, \mp x_1, 0) ; {x_1}^2 + {x_2}^2 = n \} \end{aligned}$$

である．つまり，$\mathbb{Z}^3$ にはめ込むことができる面積の n の正方形は，こんなもののしかない，ということですね．

よく見ますと，1 行目の正方形は yz 平面上，2 行目は xz 平面上，3 行目は xy 平面上に横たわっています．ということは，空間格子をつかう室内装飾をやろうとしても，**n_0 が平方因子を含まないときは，座標面でしか，そういうはめ込みができない**ということです．

これが我々の目標としていた問題の部分的解決です．

$V(n)$ を本当に決定するには，n_0 に平方因子がある場合にどうなるかを調べなければなりませんが，これはもっと難しい問題になります．

これで言いたかったことは全部言い終えました．少し長かったかもしれませんが，難しい数学は全然使っていません．みんなさんもじっくり考えてみますと，もっと短い証明ができるかもしれませんね．また条件をゆるめた場合や，正方形を三角形にしてみたり，4 次元空間にはめ込んだりして，どういうときにできて，どういうときにできないかを考えてみるとおもしろいでしょう．格子を斜めにしてみてもいいですね．

§ 13．結び(2 つの解釈)

さて，ちょっと時間があるようですので，この問題を少し上の立場から見て見ましょう．実は次の 2 つの解釈ができるのです．

［I］次のような集合を考えます．

$$W=\{(z_1, z_2, z_3)\in \mathbb{Z}[i]^3 ; {z_1}^2+{z_2}^2+{z_3}^2=0\}$$

$$\text{ただし } \mathbb{Z}[i]=\{a+ib ; a, b\in \mathbb{Z}\} \qquad (\text{ガウスの整数環}).$$

実は，この W が本質的に $\bigcup_{n=1}^{\infty} V(n)$ と同じになります[12]．

ちょっとやってみましょう．

$$z_k=x_k+iy_k \qquad (k=1, 2, 3)$$

とします．

$$ {z_k}^2={x_k}^2-{y_k}^2+2ix_ky_k. $$

$k=1, 2, 3$ として全部足してみると

$$0=Nx-Ny+2i\langle x, y\rangle.$$

実部，虚部を比べて，

$$Nx=Ny, \qquad \langle x, y\rangle=0.$$

つまり，W を実部と虚部に分けて考えたものが

$$\bigcup_{n=1}^{\infty} V(n)$$

になる，ということです(ただし，W の中で $Nx=Ny=n$ の部分が $V(n)$ に対応します)．

すなわち，我々の問題は複素数の錐面上の，ガウスの格子点についての問題と同値であるということです．複素数の上で考えれば式は 1 つになります．この場合には $\mathbb{Z}[i]$ の整数論を用いる道が開けます．これが 1 つの考察です．

12) $n=0$ のとき $V(0)=\{(0, 0)\}$ とすることはいうまでもありません．

［II］
$$X=(x,y)=\left(\begin{pmatrix}x_1\\x_2\\x_3\end{pmatrix}\begin{pmatrix}y_1\\y_2\\y_3\end{pmatrix}\right)$$

とします．行列と考え

$$X=\begin{pmatrix}x_1 & y_1\\x_2 & y_2\\x_3 & y_3\end{pmatrix}$$

として ${}^tXX$ を計算してみます．

$${}^tXX=\begin{pmatrix}{}^tx\\{}^ty\end{pmatrix}(x,y)=\begin{pmatrix}{}^txx & {}^txy\\{}^tyx & {}^tyy\end{pmatrix}=\begin{pmatrix}Nx & \langle x,y\rangle\\\langle x,y\rangle & Ny\end{pmatrix}.$$

$V(n)$ に与えた条件を思い出して

$$=\begin{pmatrix}n & 0\\0 & n\end{pmatrix}=n1_2$$

となります．我々の問題は

$${}^tX1_3X=n1_2$$

の整数解 X を全部求める，ということだったわけです．言いかえると，2 次形式の意味で次のような表現を数えあげる，という問題だったのです．

$$3\text{元}2\text{次形式}\quad 1_3\ \xrightarrow{\text{表現}}\ n1_2\quad 2\text{元}2\text{次形式}$$

こう解釈すると，有名なジーゲルの 2 次形式の基本定理というものが想い浮かびます．これは難しいものです．しかし，この定理を使ったからと言って，今やったことがすぐ出てくるかどうかは，別問題です．我々は非常にエレメンタリーなアプローチをしたわけです．

こういうふうに考えてくると，我々の室内装飾の問題も直交群の整数論あるいはさらに代数群の整数論の一部とみることもできます．この分野は世界的に見て，日本が大きく貢献しているものの 1 つです．

［1985 年 5 月 21 日，立教大学にて］

付録 3

Gauss sums and Poincaré sums (a sketch)

By Takashi Ono

Department of Mathematics, The Johns Hopkins University,
Baltimore, Maryland, 21218, U. S. A.

June 7, 2006

Abstract : colors but no sound

Key Words : Indra's Pearls

---

1. $(\mathfrak{g}, (G, M))$

Let G be a group and M be a left G-module. Consider a *finite* group $\mathfrak{g}$ which acts naturally on (G, M). In other words, we assume that G is a left $\mathfrak{g}$-group, M is a left $\mathfrak{g}$-module so that ${}^{\sigma}(sx) = {}^{\sigma}s{}^{\sigma}x$, $\sigma \in \mathfrak{g}$, $s \in G$, $x \in M$. Let c be a cocycle of $\mathfrak{g}$ in G. By definition, c is a map $\mathfrak{g} \to G$ such that $c(\sigma\tau) = c(\sigma){}^{\sigma}c(\tau)$, $\sigma, \tau \in \mathfrak{g}$. For a cocycle c, we associate a $\mathbb{Z}$-module M_c by

$$M_c = \{x \in M\,;\, c(\sigma){}^{\sigma}x = x, \sigma \in \mathfrak{g}\}. \tag{1}$$

As the group $\mathfrak{g}$ is finite, we can speak of a sum

$$p_c(x) = \sum_{\tau \in \mathfrak{g}} c(\tau){}^{\tau}x, \qquad x \in M. \tag{2}$$

We shall put

$$P_c = \{\, y = p_c(x), x \in M \,\}. \tag{3}$$

One verifies that

$$|\mathfrak{g}|M_c \subseteq P_c \subseteq M_c \tag{4}$$

---

0) 2000 Mathematics Subject Classification. 11 R 34

Dedicated to Professor S. Iyanaga, M. J. A., on his 100th birthday

where $|\mathfrak{g}|$ is the order of $\mathfrak{g}$. Denote by $Z(\mathfrak{g}, G)$ the set of all cocycles of $\mathfrak{g}$ in G. Two cocycles c, c' are equivalent $c' \sim c$ if there is a $u \in G$ such that $c'(\sigma) = u^{-1}c(\sigma)^{\sigma}u$ for some $u \in G$ for all $\sigma \in \mathfrak{g}$. One verifies that the map $x \longmapsto u^{-1}x$ induces an isomorphism of factor modules: $M_c/P_c \simeq M_{c'}/P_{c'}$. Consequently the structure of the module M_c/P_c depends only on the cohomology class $\gamma = [c]$ in the (1st) cohomology set $H^1(\mathfrak{g}, G) = Z(\mathfrak{g}, G)/\sim$.

If we put $c = 1$ in (1), (3), then we have

$$M_1 = M^{\mathfrak{g}}, \qquad P_1 = N(M)$$

and so

$$M_1/P_1 = \hat{H}^0(\mathfrak{g}, M).$$

For a general $\gamma = [c] \in H^1(\mathfrak{g}, G)$, we have a right to make identification

$$M_c/P_c = \hat{H}^0(\mathfrak{g}, M)_\gamma, \tag{5}$$

the Tate group *twisted* by γ.

In view of (5) we shall put

$$i_\gamma(\mathfrak{g}, M) = [M_c : P_c], \qquad \gamma = [c] \in H^1(\mathfrak{g}, G). \tag{6}$$

The determination of the *index* $i_\gamma(\mathfrak{g}, M)$ is our basic theme inspired by Poincaré.

In the next three sections we shall review classical cases from our view point.

---

2. Gauss sums

Let l be an odd prime, $\zeta = e^{\frac{2\pi i}{l}}$ and $K = \mathbb{Q}(\zeta)$, the l-th cyclotomic field. Denote by $\mathcal{O}$ the ring of integers of K. In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \qquad G = \mathcal{O}^\times, \qquad \mathfrak{g} = \mathrm{Gal}(K/\mathbb{Q}).$$

One knows that

$$M = \mathbf{Z}[\zeta] \simeq \mathbf{Z}^{l-1}, \qquad \mathfrak{g} \simeq \mathbf{F}_l^{\times}. \tag{7}$$

Note that one can think of $\sigma \in \mathfrak{g}$ as an element of $\mathbf{Z}$ by the reciprocity map in the second isomorphism in (7). Let us look at two famous cocycles $c \in Z(\mathfrak{g}, G)$.

(A) The *circular units* $c(\sigma) = \dfrac{1-\zeta^{\sigma}}{1-\zeta}$ form a cocycle. For this we have

$$M_c = \frac{l}{1-\zeta}\mathbf{Z} = P_c, \qquad \text{hence} \quad i_r(\mathfrak{g}, M) = 1. \tag{8}$$

(B) The *Legendre character* $c(\sigma) = \left(\dfrac{\sigma}{l}\right)$ can be thought as a cocycle (actually a homomorphism) of $\mathfrak{g}$ in G. For this we have

$$M_c = \mathbf{Z}\tau = P_c, \qquad \text{hence} \quad i_r(\mathfrak{g}, M) = 1 \tag{9}$$

where

$$\tau = \sum_{t=0}^{l-1} \left(\frac{t}{l}\right)\zeta^t,$$

the classical Gauss sum.

---

3. Theta series

For a point τ in the upper half plane, let $L_\tau = \mathbf{Z}+\mathbf{Z}\tau$ and $E_\tau = \mathbf{C}/L_\tau$, the elliptic curve over $\mathbf{C}$. Let $\mathcal{O}$ be the ring of entire functions. In accordance with notation in **1**, we set

$$M = \mathcal{O}^{+}, \qquad G = \mathcal{O}^{\times}, \qquad \mathfrak{g} = \pi_1(E_\tau) \simeq L_\tau.$$

Note that one can think of $\sigma \in \mathfrak{g}$ as $\sigma = m+n\tau$, $m, n \in \mathbf{Z}$. Let us look at the following cocycle

$$c(\sigma)(z) = \mathbf{e}\left(\frac{\tau n^2}{2} - nz\right). \tag{10}$$

For this we have

$$M_c = \mathbf{C}\vartheta_3 = P_c^*, \qquad \text{hence } i_\gamma(\mathfrak{g}, M) = 1 \tag{11}$$

where

$$\vartheta_3 = \sum_{n \in \mathbf{Z}} c(n\tau)(z).$$

the Jacobi theta series.

4. Poincaré series

This time, let $\mathcal{O}$ be the ring of holomorphic functions on the upper half plane. In accordance with notation in **1**, we set

$$M = \mathcal{O}^+, \qquad G = \mathcal{O}^\times, \qquad \mathfrak{g} = SL_2(\mathbf{Z})$$

where for $x = x(z) \in \mathcal{O}$ the group $\mathfrak{g}$ acts by the rule

$${}^\sigma x(z) = x(\sigma^{-1}z) = x\left(\frac{az+b}{cz+d}\right), \tag{12}$$

where $\sigma^{-1} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$.

For the cocycle $c(\sigma)(z) = \dfrac{1}{(cz+d)^4}$ we have

$$M_c = \left\{ x \in M\, ;\, x\left(\frac{az+b}{cz+d}\right) = (cz+d)^4 x(z), \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SL_2(\mathbf{Z}) \right\} \tag{13}$$

and

$$M_c = \mathbf{C}G_2 = P_c^*, \qquad \text{hence} \quad i_\gamma(\mathfrak{g}, M) = 1, \tag{14}$$

where

$$G_2(z) = \sum_{(m,n)\neq(0,0)} \frac{1}{(mz+n)^4}$$

the Eisenstein series of weight 4.

5. Real quadratic fields

Let $K = \mathbb{Q}(\sqrt{d})$ be a real quadratic field and $\mathcal{O}$ be the ring of integers of K. In accordance with notation in **1**, we set

$$M = \mathcal{O}^{+}, \qquad G = \mathcal{O}^{\times}, \qquad \mathfrak{g} = \mathrm{Gal}(K/\mathbb{Q}) = \langle \tau \rangle.$$

Since $\mathfrak{g}$ is cyclic, one can identify a cocycle c of $\mathfrak{g}$ in G with any element of G of norm 1. Let ε be the fundamental unit of K of norm 1 and think this as a cocycle. Hence, by (1), (3)

$$M_\varepsilon = \{x \in \mathcal{O}\ ;\ \varepsilon^\tau x = x\}, \qquad P_\varepsilon = \{x + \varepsilon^\tau x,\ x \in \mathcal{O}\}$$

and

$$i_\varepsilon(\mathfrak{g}, M) = [M_\varepsilon : P_\varepsilon] = 1 \text{ or } 2. \tag{15}$$

Here we have an interesting result due to Seok-Min Lee. Notation being as above

(i) $d \equiv 1 \pmod 4 \implies i_\varepsilon = 1,$

(ii) $d \equiv 2 \pmod 4 \implies i_\varepsilon = 2,$

(iii) $d \equiv 3 \pmod 4$ and $a_r \equiv 1 \pmod 2 \implies i_\varepsilon = 1,$

(iv) $d \equiv 3 \pmod 4$ and $a_r \equiv 0 \pmod 2 \implies i_\varepsilon = 2$

where

$$\sqrt{d} = [a_0\,;\ \overline{a_1, \cdots, a_{r-1}, a_r, a_{r-1}, \cdots, a_1, 2a_0}].$$

6. Galois extensions K/k

Let us look at the above result of S-M Lee from a general view point. We shall denote by k either a global or a local field (of characteristic 0). As such, k is either a finite extension of $\mathbb{Q}$ or $\mathbb{Q}_p$. We denote by $\mathcal{O}_k$ the ring of

integers of k.

Let K/k be a finite Galois extension with the Galois group $\mathfrak{g} = \mathrm{Gal}(K/k)$. Then $\mathfrak{g}$ acts on the ring $\mathcal{O}_K$ of integers of K and hence on the group $\mathcal{O}_K^\times$. For a cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^\times)$ we shall look at modules M_c, P_c defined by (1), (3) with $M = \mathcal{O}_K^\times$. First, viewing c as a cocycle in $Z(\mathfrak{g}, K^\times)$, we have, by *Hilbert* 90, $c(\sigma) = \xi^{-1}\,{}^\sigma\xi$ where ξ may be chosen from $\mathcal{O}_K$. Then we find that $M_c = \mathcal{O}_K \cap \xi^{-1}\mathcal{O}_k$.

In other words, we have

$$\xi M_c = \xi\mathcal{O}_K \cap \mathcal{O}_k = (\xi\mathcal{O}_K)^{\mathfrak{g}}, \qquad \xi \in \mathcal{O}_K. \tag{16}$$

Second, as $p_c(x) = \xi^{-1}\sum_{\sigma\in\mathfrak{g}} {}^\sigma\xi^\sigma x$, we have

$$\xi p_c(x) = T_{K/k}(\xi x). \tag{17}$$

From (16), (17) we obtain

$$\begin{aligned} &M_c/P_c = (\xi\mathcal{O}_K)^{\mathfrak{g}}/T_{K/k}(\xi\mathcal{O}_K) = \hat{H}^0(\mathfrak{g}, M)_\gamma, \\ &c(\sigma) = \xi^{-1}\,{}^\sigma\xi. \end{aligned} \tag{18}$$

An ideal $\mathfrak{A}$ in $\mathcal{O}_K$ will be called *ambiguous* if ${}^\sigma\mathfrak{A} = \mathfrak{A}$, $\sigma \in \mathfrak{g}$. Let $\mathfrak{p}$ be a prime ideal in $\mathcal{O}_k$. The prime decomposition of $\mathfrak{p}$ in K is of the form

$$\mathfrak{p} = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}^{e_\mathfrak{P}} = (\prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P})^{e_\mathfrak{p}}. \tag{19}$$

Let us put

$$\mathfrak{p}^\# = \prod_{\mathfrak{P}|\mathfrak{p}} \mathfrak{P}.$$

Note that (19) becomes

$$\mathfrak{p} = \mathfrak{p}^{\# e_\mathfrak{p}}. \tag{20}$$

It is easy to see that

$$\mathfrak{A} \subset \mathcal{O}_K \text{ is ambiguous} \iff \mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_\mathfrak{p}}. \tag{21}$$

For a real number x, put $\lceil x \rceil$ = the smallest integer $\geq x$. Hence when $x \notin \mathbb{Z}$, $\lceil x \rceil = [x]+1$.

Proposition 1. *Let* $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_\mathfrak{p}}$ *be an ambiguous ideal. Then we have*

$$\mathfrak{A}^{\mathfrak{g}} = \mathfrak{A} \cap \mathcal{O}_k = \prod_{\mathfrak{p}} \mathfrak{p}^{\left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil}.$$

For a Galois extension K/k of number fields or local fields, denote by $\mathcal{D}_{K/k}$ the different of the extension. It is an ambiguous integral ideal in K. So it can be expressed as

$$\mathcal{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}}. \tag{22}$$

Proposition 2. *Let* $\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}}$ *be an integral ambiguous ideal in K. Then* $T_{K/k}\mathfrak{A} = \prod_{\mathfrak{p}} \mathfrak{p}^{\left[\frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right]}$.

Since $\xi \in \mathcal{O}_K$ and $c(\sigma) \in \mathcal{O}_K^{\times}$, $\mathfrak{A} = \xi\mathcal{O}_K$ is an integral ambiguous ideal, and hence we obtain, from (18), Proposition 1, Proposition 2, the following

Proposition 3. $(M_c : P_c) = \prod_{\mathfrak{p}} N\mathfrak{p}^{\left[\frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right] - \left\lceil \frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}} \right\rceil}$, *where* $N\mathfrak{p} = (\mathcal{O}_k : \mathfrak{p})$.

From now on, let K/k be a Galois extension of number fields and $\mathfrak{g} = \mathrm{Gal}(K/k)$. Let $\mathfrak{P}$, $\mathfrak{p}$ be prime ideals of K, k, respectively such that $\mathfrak{P}|\mathfrak{p}$. Denote by $K_{\mathfrak{P}}$, $k_{\mathfrak{p}}$ the completions of K, k, respectively. Then $K_{\mathfrak{P}}/k_{\mathfrak{p}}$ is also a Galois extension whose Galois group $\mathfrak{g}_{\mathfrak{P}}$ may be identified with the decomposition group at $\mathfrak{P}$ in G. Clearly, $\mathcal{O}_K$, $\mathcal{O}_k$ are embedded in $\mathcal{O}_{K_{\mathfrak{P}}}$, $\mathcal{O}_{k_{\mathfrak{p}}}$, respectively and similarly for groups of units. Therefore, any cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^{\times})$ induces naturally a cocycle $c_{\mathfrak{P}} \in Z(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^{\times})$. Thus, we are ready to use Proposition 3 to find $(M_c : P_c)$, $(M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}})$. If ξ is a solution to the cocycle c for $\mathfrak{g}$ (see (18)), then ξ is one to the cocycle $c_{\mathfrak{P}}$ for $\mathfrak{g}_{\mathfrak{P}}$. Put

$$\mathfrak{A} = \xi\mathcal{O}_K = \prod_{\mathfrak{p}} \mathfrak{p}^{\# m_{\mathfrak{p}}} \tag{23}$$

and define

$$\mathfrak{A}_{\mathfrak{P}} = \xi\mathcal{O}_{K_{\mathfrak{P}}}. \tag{24}$$

Since

$$m_{\mathfrak{p}} = \nu_{\mathfrak{P}}(\mathfrak{A}) = \nu_{\mathfrak{P}}(\mathfrak{A}_{\mathfrak{P}})$$

the exponent $m_{\mathfrak{p}}$ for $\mathfrak{A}_{\mathfrak{P}}$ is consistent with double purposes, global and local. Next, since, by (22), we have

$$\mathscr{D}_{K/k} = \prod_{\mathfrak{p}} \mathfrak{p}^{\# t_{\mathfrak{p}}} = \prod_{\mathfrak{P}} \mathfrak{P}^{t_{\mathfrak{P}}} = \prod_{\mathfrak{P}} \mathscr{D}_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}.$$

Now, applying Proposition 3 to a local field k, we have

Proposition 4. $(M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}) = N\mathfrak{p}^{\left[\frac{m_{\mathfrak{p}}+t_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right]-\left\lceil\frac{m_{\mathfrak{p}}}{e_{\mathfrak{p}}}\right\rceil}$.

Note also that as $e_{\mathfrak{p}} = 1$, $t_{\mathfrak{p}} = 0$ for almost all $\mathfrak{p}$, the indices $(M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}}) = 1$ for almost all $\mathfrak{P}$.

Summarizing all these, we obtain

Theorem 1. *Let K/k be a finite Galois extension of number fields and $\mathfrak{g} = \mathrm{Gal}(K/k)$. For a cocycle $c \in Z(\mathfrak{g}, \mathcal{O}_K^{\times})$ denote by $c_{\mathfrak{P}}$ the cocycle induced from c by localization at $\mathfrak{P}$. Then we have the product relation $(M_c : P_c) = \prod_{\mathfrak{p}} (M_{c_{\mathfrak{P}}} : P_{c_{\mathfrak{P}}})$ where for each $\mathfrak{p}$ we choose one $\mathfrak{P}$ dividing $\mathfrak{p}$.*

From the ramification theory of Galois extensions we have

$$t_{\mathfrak{p}} \geq e_{\mathfrak{p}} - 1, \qquad \text{for all } \mathfrak{p}$$

$$t_{\mathfrak{p}} \geq 1 \iff e_{\mathfrak{p}} \geq 2 \qquad (\textit{Dedekind}).$$

Needless to say, if $e_{\mathfrak{p}} = 1$ then $\mathfrak{p}$ is unramified, if $t_{\mathfrak{p}} = e_{\mathfrak{p}} - 1 \geq 1$ then $\mathfrak{p}$ is said to be tamely ramified. Furthermore, if $\mathfrak{p}$ is such that $t_{\mathfrak{p}} \geq e_{\mathfrak{p}} \geq 2$ then $\mathfrak{p}$ is wildly ramified. (Note that $\mathfrak{p}$ is wildly ramified $\iff p | e_{\mathfrak{p}}$, where p means the characteristic of the finite field $\mathcal{O}_k/\mathfrak{p}$.)

We will use these terms for extensions in an obvious way. Proposition 4 implies immediately the following

Theorem 2. *Let K/k be a finite Galois extension of number fields. If*

K/k is unramified or tamely ramified, then $M_c = P_c$ for all cocycle $c \in Z(\mathrm{Gal}(K/k), \mathcal{O}_K^\times)$.

Since we have

$$i_\gamma(K/k) = (M_c : P_c), \qquad \gamma \in H^1(\mathfrak{g}, \mathcal{O}_K^\times) \tag{25}$$

we can express Theorem 2 as

Theorem 3. *For a finite Galois extension K/k of number fields, we have $i_\gamma(K/k) = \prod_{\mathfrak{p}} i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/k_{\mathfrak{p}})$.*

Now passing to localization, choose a prime element $\Pi \in K_{\mathfrak{P}}$. Then the relation

$$^{\sigma}\Pi = \Pi z_\sigma, \qquad \sigma \in \mathfrak{g}_{\mathfrak{P}}, \quad z_\sigma \in \mathcal{O}_{K_{\mathfrak{P}}}^\times,$$

defines the cohomology class

$$\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}} = [z] \in H^1(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times). \tag{26}$$

We know that the group $H^1(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$ is cyclic of order $e_{\mathfrak{p}}$ generated by $\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}}$. (See [2].) Therefore for any class $\gamma = [c] \in H^1(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^\times)$, a unique integer m mod $e_{\mathfrak{p}}$ is determined so that

$$\gamma = (\gamma_{K_{\mathfrak{P}}/k_{\mathfrak{p}}})^m. \tag{27}$$

In otherwords,

$$c \sim z^m. \tag{28}$$

Now, let ξ be a solution in K to the cocycle in (18). Then (28) means that

$$\frac{^{\sigma}\xi}{\xi} = u^{-1}\frac{^{\sigma}\Pi^m}{\Pi^m}{}^{\sigma}u, \qquad u \in \mathcal{O}_{K_{\mathfrak{P}}}^\times$$

or

$$u\Pi^m = \xi v \pi^r$$

where $v \in \mathcal{O}_{k_{\mathfrak{p}}}^\times$ and π being a prime element in $k_{\mathfrak{p}}$. In view of (15), we find

$$m = m_{\mathfrak{p}} + re_{\mathfrak{p}}$$

and so

$$m \equiv m_{\mathfrak{p}} \qquad \text{mod } e_{\mathfrak{p}}. \tag{29}$$

7. Quadratic fields again

Now that we have a product relation (Theorem 3), our problem of indices for global fields is entirely reduced to local computations. As the easiest example, let us look at our old works again. (See[1], [3].)

Let $K = \mathbb{Q}(\sqrt{d})$ where d is a square free integer. Let $p, \mathfrak{P}$ be primes of $\mathbb{Q}$, K, respectively, such that $\mathfrak{P}|p$. When extensions $K_{\mathfrak{P}}/\mathbb{Q}_p$ is unramified or tamely ramified, then by Proposition 4, $i_{\gamma_{\mathfrak{P}}}(K_{\mathfrak{P}}/\mathbb{Q}_p) = 1$. Therefore only wildly ramified case must be taken care of. This is precisely the case where

$$p = 2, \qquad d \equiv 2, 3 \quad \text{mod } 4.$$

(i) $p = 2$, $d \equiv 2$ mod 4. In this case, $\mathfrak{D}_{K_{\mathfrak{P}}/\mathbb{Q}_2} = \mathfrak{P}^3$ and so $t_2 = 3$. Since the order of the cohomology group $H^1(\mathfrak{g}_{\mathfrak{P}}, \mathcal{O}_{K_{\mathfrak{P}}}^{\times}) = \langle \gamma_{\mathfrak{P}}(K_{\mathfrak{P}}/\mathbb{Q}_2) \rangle$ is $e_2 = 2$, we find that the number m, in (27), is either 0 or 1. As we are allowed to replace m_2 by m mod e_2, we get, using Proposition 4,

$$i_1(K_{\mathfrak{P}}/\mathbb{Q}_2) = 2^{\left[\frac{t_2}{e_2}\right]} = 2^{\left[\frac{3}{2}\right]} = 2$$

and, for $\gamma \neq 1$,

$$i_\gamma(K_{\mathfrak{P}}/\mathbb{Q}_2) = 2^{\left[\frac{t_2+m_2}{e_2}\right]-\left[\frac{m_2}{e_2}\right]} = 2^{\left[\frac{3+1}{2}\right]-\left[\frac{1}{2}\right]} = 2.$$

So the index $i_\gamma = 2$ always.

(ii) $p = 2$, $d \equiv 3$ mod 4. In this case we have $t_2 = 2$. The similar calculation as above shows this time that

$$i_\gamma = \begin{cases} 2 & \text{when } \gamma = 1, \text{ i.e. when } m_2 \text{ is even,} \\ 1 & \text{when } \gamma \neq 1, \text{ i.e. when } m_2 \text{ is odd.} \end{cases}$$

8. Hopf map

By the Hopf map $h: \mathbb{R}^4 \longrightarrow \mathbb{R}^3$ we shall mean a map $y = h(x)$ given by a system of three quadratic forms of four variables:

$$y_1 = x_0^2 + x_1^2 - x_2^2 - x_3^2,$$
$$y_2 = 2(x_1x_2 + x_0x_3),$$
$$y_3 = 2(x_1x_3 - x_0x_2).$$

One checks that $h(S^3) \subseteq S^2$ where S^i is the unit sphere of dimension i.

Let $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$ be the division ring of the (Hamilton) quaternions and $\mathbb{H}_0$ the vector part of $\mathbb{H}$

$$\mathbb{H}_0 = \{v \in \mathbb{H}\,;\, v = x_1 i + x_2 j + x_3 k\}.$$

The *involution* on $\mathbb{H}$ is the map $x = x_0 + v \longmapsto x^* = x_0 - v$ with the well known properties. We set

$$Tx = x + x^* = 2x_0 \qquad (\textit{trace}),$$
$$Nx = xx^* = x_0^2 + x_1^2 + x_2^2 + x_3^2 \qquad (\textit{norm}).$$

We have

$$\mathbb{H}_0 = \{x \in \mathbb{H}\,;\, Tx = 0\}. \tag{30}$$

By the relation $N(xy) = NxNy$, the set $\mathbb{H}^\times = \{x \in \mathbb{H}\,;\, Nx \neq 0\}$ forms a group and hence

$$\mathbb{H}_1 = \{x \in \mathbb{H}\,;\, Nx = 1\} = S^3 \tag{31}$$

becomes its subgroup.

In terns of the involution, the Hopf map is simply

$$h(x) = xix^*, \qquad x \in \mathbb{H}. \tag{32}$$

Since $\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k = \mathbb{C} + \mathbb{C}j$, one can write

$$x = \alpha + \beta j, \qquad \alpha, \beta \in \mathbb{C}.$$

Then we find $x^* = \bar{\alpha} - \beta j$.

Call φ the map $\mathbb{H} \longrightarrow M_2(\mathbb{C})$:

$$\varphi(x) = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}.$$

Then we have

$$\varphi(x^*) = \varphi(x)^* = {}^t\overline{\varphi(x)}.$$

Consequently, an isomorphism

$$\mathbb{H}_1 \simeq SU(2). \tag{33}$$

On the other hand, φ induces an isomorphism

$$\mathbb{H}_0 \simeq \mathfrak{su}(2) = \{X \in M_2(\mathbb{C})\,;\, X^* + X = \operatorname{tr} X = 0\}. \tag{34}$$

Viewing the Hopf map h as $\mathbb{H}_1 \to \mathbb{H}_0$, we obtain

$$h(x) = xix^* = xix^{-1} = (\operatorname{Ad} x)i \tag{35}$$

and the *fibration* $0 \longrightarrow S^1 \longrightarrow S^3 \longrightarrow S^2 \longrightarrow 0$.

9. Quaternion algebras

Let F be a field of characteristic $\neq 2$. For $a, b \in F^\times$ denote by $A = (a, b)_F$ the quaternion algebra with basis $\{1, u_1, u_2, u_3\}$ with the multiplication table

$$u_iu_j = -u_ju_i \qquad (i \neq j),$$

$$u_1u_2 = u_3, \qquad u_2u_3 = -bu_1, \qquad u_3u_1 = -au_2,$$

$$u_1^2 = a, \qquad u_2^2 = b, \qquad u_3^2 = -ab.$$

Let $K = F(\sqrt{a})$. We define an F-algebra map

$$\varphi : A \to M_2(K) \tag{36}$$

by

$$u_1 \longmapsto \begin{bmatrix} \sqrt{a} & 0 \\ 0 & -\sqrt{a} \end{bmatrix}, \qquad u_2 \longmapsto \begin{bmatrix} 0 & 1 \\ b & 0 \end{bmatrix}, \qquad u_3 \longmapsto \begin{bmatrix} 0 & \sqrt{a} \\ -b\sqrt{a} & 0 \end{bmatrix}.$$

To be precise, we have

$$\varphi(x) = \begin{bmatrix} x_0 + x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & x_0 - x_1\sqrt{a} \end{bmatrix}.$$

In A we have an involution $x \longmapsto x^*$, Tx and Nx, as in **8** which are compatible with the usual notation in linear algebra via the map φ. For example equalities like

$$Tx = \mathrm{tr}\ x = 2x_0,$$
$$Nx = \det\ x = x_0^2 - ax_1^2 - bx_2^2 + abx_3^2$$

make sense.

Again as in **8**, we define A_0, A_1 for $A = (a, b)_F$:

$$A_0 = \{ x \in A \,;\, Tx = 0 \} = \left\{ x = \begin{bmatrix} x_1\sqrt{a} & x_2 + x_3\sqrt{a} \\ b(x_2 - x_3\sqrt{a}) & -x_1\sqrt{a} \end{bmatrix} \right\} \tag{37}$$

$$A_1 = \{ g \in A \,;\, Ng = 1 \} = \{ g \in A \,;\, \det g = 1 \}. \tag{38}$$

A_1 is a group acting on the vector space A_0 over F by

$$g \circ x = gxg^{-1} = gxg^*. \tag{39}$$

Lemma 1. *For $x \in A$, $x \neq 0$, we have*

$$x \in A_0 \iff x^2 \in F \text{ and } x \notin F.$$

10. Case $K = \mathbb{Q}$

Let $A = (a, b)_F$ be quaternion algebra as in **9**. Since $K = F(\sqrt{a})$ we have two cases : $K = F$ or $[K : F] = 2$. From now on, we shall assume that $F = \mathbb{Q}$. So either $K = \mathbb{Q}$ or $K = \mathbb{Q}(\sqrt{a})$. In this section, we assume, for simplicity, that $a = b = 1$. The map φ in (36) boils down to

$$A = (1, 1)_{\mathbb{Q}} \simeq M_2(\mathbb{Q}) \tag{40}$$

given by

$$x \longmapsto \varphi(x) = \begin{bmatrix} x_0+x_1 & x_2+x_3 \\ x_2-x_3 & x_0-x_1 \end{bmatrix}.$$

Now set

$$A(\mathbb{Z}) = \varphi^{-1}(M_2(\mathbb{Z})). \tag{41}$$

In other words, via φ, one can write $A(\mathbb{Z}) = M_2(\mathbb{Z})$. Then set

$$A_0(\mathbb{Z}) = A_0 \cap A(\mathbb{Z}).$$

From (40), we infer that

$$A_0(\mathbb{Z}) = \{\, x = \begin{bmatrix} h & k \\ l & -h \end{bmatrix},\ h, k, l \in \mathbb{Z} \,\}. \tag{42}$$

For a square free integer m, set

$$\begin{aligned} S(m) &= \{x \in A_0(Z)\,;\, \det x = m\} \\ &= \{x \in A(\mathbb{Z}),\ \mathrm{tr}\, x = 0,\ \det x = m\}. \end{aligned} \tag{43}$$

For $x \in S(m)$, its characteristic polynomial is $f(t) = t^2+m \in \mathbb{Z}[t]$. In general, for a polynomial $f \in \mathbb{Z}[t]$ put

$$M_2(\mathbb{Z}, f) = \{x \in M_2(\mathbb{Z})\,;\, f(x) = 0\}.$$

Then we have

Lemma 2. $S(m) = M_2(\mathbb{Z}, t^2+m)$.

Now the group $G = GL_2(\mathbb{Z})$ acts on $S(m)$ by $g\circ x = gxg^{-1}$. Let us denote the orbit space by

$$S(m)/G.$$

By Lemma 2, we have $S(m)/G = M_2(\mathbb{Z}, t^2+m)/G$. On the other hand, it follows from a well known theorem that one has a bijection

$$M_2(\mathbb{Z}, t^2+m)/G \simeq I(\mathbb{Z}[\sqrt{-m}])/G \tag{44}$$

where $I(\mathbb{Z}[\sqrt{-m}])$ means the set of all ideals of the order $\mathbb{Z}[\sqrt{-m}]$.

If, in particular, $m \equiv 1, 2 \mod 4$, then $I(\mathbb{Z}[\sqrt{-m}]))$ is the maximal order of K and , by Lemma 2, we obtain

$$|S(m)/G| = h(\sqrt{-m}),$$

the class number of the quadratic field $\mathbb{Q}(\sqrt{-m})$.

11. Case $K = \mathbb{Q}(\sqrt{a})$

Let $A = (a, b)_{\mathbb{Q}}$. We assume now that $K = \mathbb{Q}(\sqrt{a})$ is a quadratic field. From now on we set

$$\theta = \sqrt{a}.$$

We denote by $\mathcal{O}$ the ring of integers of K. We find it convenient to assume that $a \equiv 2, 3 \bmod 4$ so that

$$\mathcal{O} = \mathbb{Z}[\theta].$$

The Galois group $\mathfrak{g}$ of $K/\mathbb{Q}$ is cyclic of order 2 ; the unique generator will be given by $x \longmapsto \bar{x}$. For example,

$$\bar{\theta} = -\theta.$$

Finally, for simplicity, we assume that

$$b = -1.$$

The map φ in (36) goes like

$$A = (a, -1)_{\mathbb{Q}} \longrightarrow M_2(K) \tag{45}$$

with

$$x = x_0 + x_1 u_1 + x_2 u_2 + x_3 u_3 \longmapsto \varphi(x) = \begin{bmatrix} x_0 + x_1\theta & x_2 + x_3\theta \\ -x_2 + x_3\theta & x_0 - x_1\theta \end{bmatrix}.$$

For integral points of A, we set, as in (41)

$$A(\mathbb{Z}) = \varphi^{-1}(M_2(\mathcal{O})) = \{x = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \in M_2(\mathcal{O})\}. \tag{46}$$

Furthermore, we set

$$A_1(\mathbb{Z}) = \{g = \begin{bmatrix} \alpha & \beta \\ -\bar{\beta} & \bar{\alpha} \end{bmatrix}; \alpha, \beta \in \mathcal{O},\ \det g = \alpha\bar{\alpha} + \beta\bar{\beta} = 1\} \tag{47}$$

$$A_0(\mathbb{Z}) = \{x = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix}; z, w \in \mathcal{O},\ \mathrm{tr}\ x = z + \bar{z} = 0\}. \tag{48}$$

In accordance with notation in **1**, we set

$$M = A_0(\mathbb{Z}), \qquad G = A_1(\mathbb{Z}), \qquad \mathfrak{g} = \mathrm{Gal}(K/\mathbb{Q})$$

Let us study the cohomology set $H^1(\mathfrak{g}, G)$. As explained in the beginning of **5**, we have

$$Z^1(\mathfrak{g}, G) = \{ c = \begin{bmatrix} z & w \\ -\bar{w} & \bar{z} \end{bmatrix} \in G,\ c\bar{c} = 1 \} \tag{49}$$

and

$$c' \sim c,\ c, c' \in Z^1(\mathfrak{g}, G) \iff c' = g^{-1}c\bar{g},\ \exists\, g \in G. \tag{50}$$

The following lemma follows from our assumption $b = -1$.

Lemma 3. $\bar{g} = u_2 g u_2^{-1}, \qquad u_2 = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$

We set

$$S = A_1(\mathbb{Z}) \cap A_0(\mathbb{Z}) = \{s \in A(\mathbb{Z})\,;\, \mathrm{tr}\ s = 0,\ \det\ s = 1\}. \tag{51}$$

Note that $u_2 \in S$.

Lemma 4. $Z^1 u_2 = S$.

Theorem 4. *Let* $A = (a, -1)_{\mathbb{Q}}$ *where a is a square free integer such that* $a \equiv 2, 3 \bmod 4$. *Let* $S = A_1(\mathbb{Z}) \cap A_0(\mathbb{Z})$ *and* $\mathfrak{g} = \mathrm{Gal}(\mathbb{Q}(\sqrt{a})/\mathbb{Q})$. *Then we have* $H^1(\mathfrak{g}, A_1(\mathbb{Z})) \simeq S/A_1(\mathbb{Z})$.

Remark 1. *To know the set* $H^1(\mathfrak{g}, A_1(\mathbb{Z}))$ *is, of course, necessary to study thoroughly our system* $(\mathfrak{g}, (G, M))$ *in* **1**. *We hope to come back to this problem sometime soon.*

● **References**

[1] Ono, T.: A Note on Poincaré sums for finite groups. Proc. Japan Acad., **79A**, 95-97 (2003).

[2] Ono, T.: On Poincaré sums for local fields. Proc. Japan Acad., **79A**, 115-118 (2003).

[3] Lee, S-M, and Ono, T.: On a certain invariant for real quadratic fields. Proc. Japan Acad., **79A**, 119-122 (2003).

[4] Ono, T : On Poincaré sums for number fields. Proc. Japan Acad., **81A**, 65-68 (2005).

[5] Cassels, J. W. S., and Fröhlich, A. (eds.) : Algebraic Number Theory (Proc. Instructional Conf., Brighton, 1965). Academic Press, London-New York (1967).

索引

●さ行

●た行

●な行

●は行

●ま行

●や行

●ら行

小野 孝(おの・たかし)

略歴

1928 年　兵庫県西宮市に生まれる.
1952 年　東京大学理学部数学科を卒業.
その後, 名古屋大学, 大阪市立大学, ポアンカレ研究所(パリ), 高級研究所(プリンストン), ブリティッシュ・コロンビア大学, ペンシルヴァニア大学を経て,
現　在　ジョンズ・ホプキンス大学教授. 専門は数論. 理学博士.

主な著書

『数論序説』裳華房
『オイラーの主題による変奏曲』実教出版
『代数群の整数論とその応用』立教大学
《An Introduction to Algebraic Number Theory》Plenum
《Variations on a Theme of Euler》Plenum

ガウスの和 ポアンカレの和——数論の最前線から

2008 年 4 月 15 日　第 1 版第 1 刷発行

著　者……………………………小野　孝 ©
発行者……………………………林　克行
発行所……………………………株式会社 日本評論社
〒170-8474 東京都豊島区南大塚 3-12-4
電話：03-3987-8621［販売部］　http://www.nippyo.co.jp
企画・制作………………………亀書房［代表：亀井哲治郎］
〒264-0032 千葉市若葉区みつわ台 5-3-13-2
電話 & FAX：043-255-5676
http://homepage 2.nifty.com/kame-shobo/
印刷所……………………………精文堂印刷株式会社
製本所……………………………牧製本印刷株式会社
装　幀……………………………駒井佑二
ISBN 978-4-535-78532-8　Printed in Japan